

2002-269271

[Title of the Invention] CERTIFICATE ISSUANCE SYSTEM AND
CERTIFICATE ISSUANCE APPARATUS

[Abstract]

[Problem to be solved] To prevent an agent or the like from forging a certificate by illegally using vouchers.

[Solution] Terminals 2 each having a printing material 3 such as paper for issuing a certificate and a certificate management server 4 for managing the printing material 3 are connected to each other through a network 5. Each terminal 2 reads the identification information 31 attached to the printing material 3 and sends the identification information 31 to the certificate management server 4, which confirms whether the identification information 31 is legitimate or not. The terminal 2 then issues a certificate by recording the contents of the certificate on the printing material 3.

[Scope of Claim for a Patent]

[Claim 1] A certificate issuance system:

wherein at least a terminal for reading the identification information of a recording medium attached to a printing material and a certificate management server for managing the recording medium are connected to each other through a network;

wherein each terminal includes an identification information reading means for reading the identification information of the recording medium and an identification information transmission means for transmitting the identification information to the certificate management server;

wherein the certificate management server includes an identification information database for managing the identification information and an authenticity transmission means for transmitting authenticity information indicating, based on the identification information whether the recording medium is genuine or not to the terminal; and

wherein each terminal includes a certificate issuance means for issuing a certificate by printing the contents of the certificate on the printing material in the case where the authenticity information is genuine.

[Claim 2] The certificate issuance system as set forth in claim 1,

characterized in that the recording medium is an IC chip having stored therein the identification information.

[Claim 3] The certificate issuance system as set forth in claim 1 or 2,

characterized in that the certificate issuance means stores the contents of the certificate in the recording medium.

[Claim 4] A certificate issuance system:

wherein at least a terminal for reading the identification information of a recording medium attached to a printing material and a certificate management server for managing the recording medium are connected to each other through a network; and

wherein the terminal includes:

an identification information reading means for reading the identification information of the recording medium;

an identification information transmission means for transmitting the identification information to the certificate management server;

an authenticity receiving means for receiving the authenticity information indicating whether the recording medium is legitimate or not from the certificate management server; and

a certificate issuance means for judging that the recording medium is legitimate and, by printing the contents of a certificate on the printing material, issuing the certificate in the case where the authenticity information is genuine.

[Claim 5] A certificate issuance system:

wherein at least a terminal for reading the

identification information of a recording medium attached to a printing material and a certificate management server for managing the recording medium are connected to each other through a network; and

wherein the certificate management server includes:

an identification information receiving means for receiving the identification information of the recording medium from the terminal;

an identification information database for managing the identification information;

an authenticity judging means for retrieving the identification information from the identification information database and judging the authenticity as to whether the identification information is legitimate or not; and

an authenticity transmission means for transmitting to the terminal authenticity information to allow the terminal to issue a certificate in the case where the authenticity information is genuine.

[Claim 6] A certificate issuance system:

wherein at least a terminal for reading the identification information of a recording medium and a certificate management server for managing the recording medium are connected to each other through a network;

wherein the terminal includes an identification information reading means for reading the identification information of the recording medium and an identification information transmission means for transmitting the

identification information to the certificate management server;

wherein the certificate management server includes an identification information database for managing the identification information and an authenticity transmission means for transmitting the authenticity information indicating, based on the identification information whether the recording medium is legitimate or not to the terminal; and

wherein the terminal includes a certificate issuance means for issuing a certificate by recording the contents of the certificate on the recording medium in the case where the authenticity information is genuine.

[Claim 7] The certificate issuance system as set forth in claim 6,

characterized in that the recording medium is an IC card having stored therein the identification information.

[Claim 8] A certificate issuance system:

wherein at least a terminal for reading the identification information of a recording medium and a certificate management server for managing the recording medium are connected to each other through a network; and

wherein the terminal includes:

an identification information reading means for reading the identification information of the recording medium;

an identification information transmission means for transmitting the identification information to the certificate management server;

an authenticity receiving means for receiving the authenticity information indicating whether the recording medium is legitimate or not from the certificate management server; and

a certificate issuance means for judging that the recording medium is legitimate and issuing a certificate by recording the contents of the certificate on the recording medium in the case where the authenticity information is genuine.

[Claim 9] A certificate issuance system:

wherein at least a terminal for reading the identification information of a recording medium and a certificate management server for managing the recording medium are connected to each other through a network; and

wherein the certificate management server includes:

an identification information receiving means for receiving the identification information of the recording medium from the terminal;

an identification information database for managing the identification information;

an authenticity judging means for retrieving the identification information from the identification information database and judging whether the identification information is genuine or not; and

an authenticity transmission means for transmitting to the terminal authenticity information to allow the terminal to issue a certificate in the case where the authenticity

information is genuine.

[Claim 10] A certificate issuance apparatus comprising:

an identification information reading means for reading the identification information of a recording medium attached to a printing material;

an identification information database for storing the identification information;

an authenticity judging means for judging an authenticity by searching the identification information database as to whether the identification information is legitimate or not; and

a certificate issuance means for issuing a certificate by printing the contents of the certificate on the printing material in the case where the authenticity information is genuine.

[Claim 11] A certificate issuance apparatus comprising:

an identification information reading means for reading the identification information of a recording medium;

an identification information database for storing the identification information;

an authenticity judging means for judging an authenticity by searching the identification information database as to whether the identification information is legitimate or not; and

a certificate issuance means for issuing a certificate by recording the contents of the certificate on the recording medium in the case where the authenticity information is

genuine.

[Detailed Description of the Invention]

[0001]

[Technical Field of the Invention] The present invention relates to a certificate issuance system for issuing a certificate.

[0002]

[Prior Art] Conventionally, for mandatory automobile liability insurance or the like, a bundle of five vouchers handwritten by an agent or partly printed on a dot printer from an office computer is issued as a certificate. This certificate can be canceled whenever it become unrequired due to the scrapping or the like and a surrender value can be received with the cancellation.

[0003]

[Problem to be Solved by the Invention] Thus, an agent or the like can receive the surrender value by forging the vouchers illegally. In order to prevent the forgery, the vouchers are required to be kept under control. For example, the number of the vouchers deposited in an agent is managed and the vouchers are collected at intervals of several months by the insurance company. The sum of the number of applications for the mandatory automobile liability insurance filed by the agent and the number of the remaining vouchers is required to coincide with the initial number of vouchers deposited in the agent. Also, the vouchers miswritten, if any, by the agent are required to be kept in hand. This is not only a very bothersome job,

but also the collection and the miswriting cause the wasteful disposal of about 30 to 40 % of the blank vouchers distributed from the insurance company.

[0004]

[Means for Solving the Problem] In order to solve the problem described above, according to claim 1 of the invention, there is provided a certificate issuance system: wherein at least a terminal for reading the identification information of a recording medium attached to a printing material, and a certificate management server for managing the recording medium are connected to each other through a network; wherein each terminal includes an identification information reading means for reading the identification information of the recording medium and an identification information transmission means for transmitting the identification information to the certificate management server; wherein the certificate management server includes an identification information database for managing the identification information and an authenticity transmission means for transmitting the authenticity information indicating, based on the identification information whether the recording medium is genuine or not to the terminal; and wherein each terminal includes a certificate issuance means for issuing a certificate by printing the contents of the certificate on the printing material in the case where the authenticity information is genuine.

[0005] In the configuration described above, the terminal for issuing a certificate on the printing material constituting a

printable material such as paper having attached thereto the recording medium such as an IC card or a magnetic card and a magnetic portion such as an IC chip or a magnetic card contained in the IC card as the recording medium and the certificate management server for managing the identification information recorded in the recording medium are connected to each other through a network, the terminal reads the identification information stored in the recording medium to issue a certificate and transmits the identification information to the certificate management server to confirm whether the recording medium is legitimate or not, and in the case where the recording medium is legitimate, the terminal issues a certificate by printing the contents of the certificate on the printing material. The certificate is a concept including the insurance policy or documents, a copy of the family register and the certificate of residence.

[0006] According to claim 2, there is provided the certificate issuance system as set forth in claim 1, characterized in that the recording medium is an IC chip having stored therein the identification information.

[0007] In the configuration described above, the recording medium is an IC chip and can store the identification information.

[0008] According to claim 3, there is provided the certificate issuance system as set forth in claim 1 or 2, characterized in that the certificate issuance means stores the contents of the certificate in a recording medium.

[0009] In the configuration described above, not only the certificate is printed but also the contents of the certificate can be recorded on the recording medium as required.

[0010] According to claim 4, there is provided a certificate issuance system: wherein at least a terminal for reading the identification information of a recording medium attached to a printing material and a certificate management server for managing the recording medium are connected to each other through a network; wherein the terminal includes an identification information reading means for reading the identification information of the recording medium, an identification information transmission means for transmitting the identification information to the certificate management server, an authenticity receiving means for receiving the authenticity information indicating whether the recording medium is legitimate or not from the certificate management server, and a certificate issuance means for judging that the recording medium is legitimate and, by printing the contents of a certificate on the printing material, issuing the certificate in the case where the authenticity information is genuine.

[0011] In the configuration described above, the terminal reads the identification information stored in the recording medium such as the IC chip or the magnetic card (magnetic portion) attached to the printing material such as paper to issue a certificate, the certificate management server confirms whether the recording medium is legitimate or not, and in the

case where the recording medium is legitimate, the terminal issues a certificate by printing the contents of the certificate on the printing material such as paper.

[0012] According to claim 5, there is provided a certificate issuance system: wherein at least a terminal for reading the identification information of a recording medium attached to a printing material and a certificate management server for managing the recording medium are connected to each other through a network; and wherein the certificate management server includes an identification information receiving means for receiving the identification information of the recording medium from the terminal, an identification information database for managing the identification information, an authenticity judging means for retrieving the identification information from the identification information database and judging the authenticity as to whether the identification information is legitimate or not, and an authenticity transmission means for transmitting to the terminal the authenticity information to allow the terminal to issue a certificate in the case where the authenticity information is genuine.

[0013] In the configuration described above, the certificate management server searches the identification information database based on the received identification information to confirm whether the recording medium attached to the printing material such as paper is legitimate or not, and in the case where the recording medium is legitimate, transmits the

authenticity information to the terminal to allow the terminal to print the contents of the certificate on the printing material.

[0014] According to claim 6, there is provided a certificate issuance system: wherein at least a terminal for reading the identification information of a recording medium and a certificate management server for managing the recording medium are connected to each other through a network; wherein the terminal includes an identification information reading means for reading the identification information of the recording medium and an identification information transmission means for transmitting the identification information to the certificate management server; wherein the certificate management server includes an identification information database for managing the identification information and an authenticity transmission means for transmitting the authenticity information indicating, based on the identification information whether the recording medium is legitimate or not to the terminal; and wherein the terminal includes a certificate issuance means for issuing a certificate by recording the contents of the certificate on the recording medium in the case where the authenticity information is genuine.

[0015] In the configuration described above, the terminal for issuing a certificate on the recording medium such as an IC card or a magnetic card and a certificate management server for managing the recording medium are connected to each other through a network, the terminal reads the identification

information stored in the recording medium for issuing the certificate and transmits the identification information to the certificate management server, which confirms whether the recording medium is legitimate or not, and in the case where the recording medium is legitimate, the terminal issues the certificate by recording the contents of the certificate on the recording medium such as the IC card or the magnetic card.

[0016] According to claim 7, there is provided the certificate issuance system as set forth in claim 6, characterized in that the recording medium is an IC card having stored therein the identification information.

[0017] In the configuration described above, the IC card can be issued as a certificate.

[0018] According to claim 8, there is provided a certificate issuance system: wherein at least a terminal for reading the identification information of a recording medium and a certificate management server for managing the recording medium are connected to each other through a network; and wherein the terminal includes an identification information reading means for reading the identification information of the recording medium, an identification information transmission means for transmitting the identification information to the certificate management server, an authenticity receiving means for receiving the authenticity information indicating whether the recording medium is legitimate or not from the certificate management server, and a certificate issuance means for judging that the recording medium is legitimate and issuing a

certificate by recording the contents of the certificate on the recording medium in the case where the authenticity information is genuine.

[0019] In the configuration described above, the terminal reads the identification information stored in a recording medium such as an IC chip or a magnetic card (magnetic portion), the certificate management server confirms whether the recording medium is legitimate or not, and in the case where the recording medium is legitimate, the terminal issues the certificate by recording the contents of the certificate on the recording medium.

[0020] According to claim 9, there is provided a certificate issuance system: wherein at least a terminal for reading the identification information of a recording medium and a certificate management server for managing the recording medium are connected to each other through a network; and wherein the certificate management server includes an identification information receiving means for receiving the identification information of the recording medium from the terminal, an identification information database for managing the identification information, an authenticity judging means for retrieving the identification information from the identification information database and judging whether the identification information is genuine or not; and an authenticity transmission means for transmitting to the terminal the authenticity information to allow the terminal to issue a certificate in the case where the authenticity

information is genuine.

[0021] In the configuration described above, the certificate management server searches the identification information database according to the received identification information, confirms whether the recording medium such as an IC chip or a magnetic card (magnetic portion) is legitimate or not, and in the case where the recording medium is legitimate, transmits the authenticity information to the terminal for allowing the terminal to record the contents of the certificate on the printing material.

[0022] According to claim 10, there is provided a certificate issuance apparatus comprising an identification information reading means for reading the identification information of a recording medium attached to a printing material, an identification information database for storing the identification information, an authenticity judging means for judging the authenticity by searching the identification information database as to whether the identification information is legitimate or not, and a certificate issuance means for issuing a certificate by printing the contents of the certificate on the printing material in the case where the authenticity information is genuine.

[0023] In the configuration described above, the identification information of the recording medium such as an IC chip or a magnetic card (magnetic portion) attached to a printing material such as paper is read to confirm whether the printing material is legitimate or not based on the

identification information, and in the case where the recording medium is legitimate, the certificate is issued by printing the contents of the certificate on the printing material.

[0024] According to claim 11, there is provided a certificate issuance apparatus comprising an identification information reading means for reading the identification information of a recording medium, an identification information database for storing the identification information, an authenticity judging means for judging the authenticity by searching the identification information database as to whether the identification information is legitimate or not, and a certificate issuance means for issuing a certificate by recording the contents of the certificate on the recording medium in the case where the authenticity information is genuine.

[0025] In the configuration described above, the identification information of the recording medium such as an IC chip or a magnetic card (magnetic portion) is read, and based on the identification information, whether the printing material is legitimate or not is confirmed, and in the case where the recording medium is legitimate, the certificate is issued by printing the contents of the certificate on the recording medium.

[0026]

[Mode for Carrying out the Invention] Embodiments of the present invention are described below with reference to the drawings. Fig. 1 is a diagram showing the configuration of a

certificate issuance system 1 of the invention. The certificate issuance system 1 includes a terminal 2 for issuing a certificate by printing the certificate on a printing material 3 having attached thereto a recording medium 31 prepared in advance, a certificate management server 4 for managing the recording medium and a network 5. The identification information is stored in the recording medium 31, and the certificate management server 4 has an identification information database 41 for managing the identification information. This embodiment is described below with reference to a case in which the terminal 2 is installed in a shop such as a convenience store or an agent to issue the insurance policy for the mandatory automobile liability insurance or the like. Also, the printing material 3 with the recording medium 31 attached thereto is distributed to the shop such as the convenience store or the agent from an organization issuing the certificate on behalf of an insurance company.

[0027] The printing material 3 with the recording medium 31 attached thereto, as an example thereof shown in Fig. 2, is typically paper to which the recording medium 31 such as an IC chip, a magnetic card (magnetic portion), a bar-code or a hologram is attached. Specifically, it is the paper with a built-in semiconductor such as an IC chip, the paper with a magnetic card (magnetic portion) attached thereto or the paper printed with a bar-code or a hologram. The IC chip, configured of a CPU and a memory, has the function as a computer. Also, the IC chip has an antenna capable of input/output without

contact, or has an IC chip with a terminal for input/output by contact.

[0028] The identification information is uniquely assigned by the insurance company or the like organization issuing the certificate and formed of a randomly assigned number or an encrypted data. Also, the identification information is stored in the magnetic portion of the magnetic card or the semiconductor such as the IC chip (contact or noncontact type). As an alternative, it is contained as information in a bar-code or a hologram. The data is preferably stored in the semiconductor such as the IC chip not in a rewritable way.

[0029] The terminal 2 is, as shown in Fig. 3, for example, is arranged inside a counter 7 of a shop such as a convenience store and so configured that a printing unit 200 such as a printer with an identification information reader 204 is connected to a computer 203 such as a personal computer so that the data is transmitted to or received from the certificate management server 4 using the communication function of the computer 203. Also, the printing unit 200, as shown in Fig. 4, includes a printing section 201, the identification information reader 204 and a communication unit 202 connected to the computer 203.

[0030] The identification information reader 204 is a unit for reading the identification information stored in various recording media 3 and constituted of an IC card reader (including a means for reading from an IC chip), a magnetic data reader, a hologram reader or a bar-code reader.

[0031] In the case where the contents of the certificate are

added to the recording medium 31, the printing unit 200 may be configured of an IC card writing unit (including a means for writing to an IC chip) or a magnetic card writing unit.

[0032] The terminal 2, as shown in Fig. 5, may be so configured that the printing unit 200 such as a printer is arranged inside the counter 7 of a shop like a convenience store and the communication unit 202 has the function of transmitting and receiving data to and from the certificate management server 4.

[0033] As an alternative, the certificate may be issued by a multi-function information terminal which may be installed in a convenience store or the like.

[0034] The certificate management server 4 is a computer having a central processing unit such as a CPU, a memory such as a RAM or a ROM and a communication unit. Further, the certificate management server 4 includes an identification information database 41 for managing identification information 32 of the recording medium 31. The communication unit has the function of transmitting and receiving the data to and from the network 5.

[0035] The network 5 connecting the terminal 2 and the certificate management server 4 can take any of various channel forms including a dedicated line, a public line such as ISDN and radio communication. Further, the internet may be used in the configuration. To secure the reliability of information management, however, a network having a high security is desired.

[0036] Next, the function of the certificate issuance system 1 is explained with reference to the block diagram of Fig. 6. The terminal 2 includes an identification information reading means 26 having the identification information reader 204 for reading the identification information 32 stored in the recording medium 31 such as an IC chip, an identification information transmission means 27 for transmitting the identification information 32 to the certificate management server 4, an authenticity receiving means 28 for receiving, from the certificate management server 4, authenticity information 33 indicating whether the identification information 32 is legitimate or not, and a certificate issuance means 29 for issuing a certificate using the printing unit 200.

[0037] The certificate management server 4 includes the identification information database 41 for managing the identification information 32 of the recording medium 3 distributed, an identification information receiving means 42 for receiving the identification information 32 from the terminal 2, an authenticity judging means 43 for judging the authenticity of the identification information by searching the identification information database 41 to check whether the identification information 32 is in the identification information database 41 or not, and an authenticity transmission means 44 for transmitting the authenticity information indicating the authenticity to the terminal 2. The authenticity judging means 43 may also be configured to execute the decryption process in the case where the identification

information is encrypted.

[0038] Next, the operation of the certificate issuance system 1 is explained with reference to the flowchart shown in Fig. 7. A case is taken up in which an insurance company issues a certificate of the mandatory automobile liability insurance or the like using the paper (printing material) 3 with a built-in IC chip (recording medium 31). In the case, the terminal 2 is installed inside the counter 7 of a shop such as a convenience store and issues the certificate using the printing unit 200 such as a printer from the computer 203 such as a personal computer. Further, in this case, the noncontact-type IC chip is used as the recording medium 31, and the IC card reader as the identification information reader 204.

[0039] First, the paper 3 with the built-in IC chip 31 is distributed from the insurance company to the shop such as a convenience store. The insurance company stores the identification information 32 in the IC chip 31 in advance. The paper 3 with the built-in IC chip 31 is set in the printing unit 200 installed inside the counter of the shop.

[0040] Assume that the customer applies for the mandatory automobile liability insurance and that upon completion of the application, the payment of the insurance money is confirmed (the withdrawal is confirmed in the case of the credit card is used). An instruction to issue a certificate is then sent from the computer 203 to the printing unit 200. The printing unit 200, upon receipt of the instruction to issue the certificate, is supplied with the paper 3 with the built-in IC chip 31, and

an instruction to read the identification information 32 is transmitted to the IC chip 31 from the IC card reader (identification information reading unit) 204 of the identification information reading means 26. The identification information 32 is sent from the IC chip 31 and received by the IC card reader 204 (S100). The identification information transmission means 27 transmits the received identification information 32 from the communication unit 23 to the certificate management server 4 (S101).

[0041] In the certificate management server 4, the identification information receiving means 42 receives the identification information 32 (S200), and the authenticity judging means 43 searches the identification information database for the identification information 32 (S201) and judges whether the identification information 32 is legitimate or not. The identification information 32, if encrypted, is decrypted and retrieved from the identification information database 41 (S201) thereby to judge whether the identification information 32 is legitimate or not. In the case where the identification information 32 is legitimate (S202), the authenticity information 33 is determined as genuine (S205), while in the case where the identification information 32 is not legitimate (S204), the authenticity information 33 is determined as false (S205). Further, the authenticity transmission means 44 transmits the authenticity information 33 to the terminal 2.

[0042] The authenticity receiving means 28 of the terminal 2

receives the authenticity information 33 through the communication unit 23 (S102), and in the case where the authenticity information 33 is genuine (S103), the certificate issuance means 29 issues the certificate by printing the contents of the certificate on the paper 3 with the built-in IC chip using the printing unit 200 (S104). In the case where the authenticity information 33 is false (S103), on the other hand, an error is displayed (S106).

[0043] Further, at the end of printing the certificate, the fact that the certificate is issued is transmitted to the certificate management server 4 (S105). The certificate management server 4 receives the notice that the certificate is already issued (S206) and the identification information 32 stored in the identification information database 41 is set as issued (S207).

[0044] In printing the certificate on the paper 3 with the built-in IC chip 31, the IC card writer may be provided on the printing unit to write the required information in the IC chip 31.

[0045] As explained above, the certificate of the mandatory automobile liability insurance or the like can be printed only on the paper distributed from the insurance company based on the identification information 32.

[0046] Also, at the time of paying the insurance money or the surrender value due to the scrapping according to the mandatory automobile liability insurance, the information (including the identification information) stored in the IC chip may be read

to confirm that the certificate is legitimate.

[0047] The noncontact-type IC chip explained above may be replaced with the contact-type IC chip. In that case, the IC chip reader/writer is configured in such a manner that the position for reading/writing the IC chip can be fixed. As an alternative, also at the time of using the magnetic card, the magnetic card reader/writer is configured in such a manner that the position of reading/writing the magnetic card can be fixed.

[0048] Further, the paper or the like printing material with the identification information 32 printed as a bar-code or a hologram thereon may be used, in which case the identification information reader 204 is a bar-code reader or a hologram reader.

[0049] As explained in detail above, according to the first embodiment, the identification information attached to the printing material such as paper is confirmed, and by thus judging whether the identification information is a legitimate one distributed from the insurance company, the certificate of the mandatory automobile liability insurance or the like can be printed.

[0050] Next, according to a second embodiment, an explanation is given about a case in which the certificate is issued by the recording medium 31. The same component parts as those in the aforementioned embodiment are designated by the same reference numerals, respectively, and not described in detail any further. Fig. 8 shows the configuration of the certificate issuance system 1 according to the second embodiment. In the second

embodiment, the terminal 2 issues the certificate is issued in the form of the recording medium 31 such as an IC card with a built-in IC chip.

[0051] The terminal 2 is configured, as an example, in such a manner that as shown in Fig. 9, the computer 203 such as the personal computer is connected with a recording medium reader/writer 200' such as an IC card reader/writer, and by utilizing the communication function of the computer 203, the data is transmitted to and received from the certificate management server 4.

[0052] According to the second embodiment, the function of the certificate issuance system 1 is explained with reference to the block diagram of Fig. 10. In the identification information reader 26 of the terminal 2, the recording medium reader/writer 200' such as the IC card reader/writer reads the identification information 32 stored in the recording medium 31 such as an IC card, and the certificate issuance means 29 issues the certificate using the recording medium reader/writer 200' such as the IC card reader/writer.

[0053] The recording medium 31 may be a plastic card with a built-in IC chip, a magnetic card with the magnetic tape attached to a plastic card, an optical disk such as CD-ROM, CD-RW, or a magnetic medium such as MO, MD or FD. This recording medium 31 is uniquely assigned the identification information 32 by an organization such as an insurance company issuing the certificate, and the contents of the certificate are additionally written in the recording medium 31 and then issued

as a certificate.

[0054] The description that follows represents a case in which the IC card (recording medium) 31 is issued as a certificate. The IC card 31, as shown in Fig. 11, is formed of a plastic card with a built-in IC module 311. The IC module 311 is configured of an IC chip 313 having a terminal 312 for data input/output. The IC card reader inputs/outputs the data after being brought into contact with the terminal 312 or without contact with the terminal 312 acting as an antenna.

[0055] The operation of the certificate issuance system 1 different from the operation of the aforementioned embodiment is explained with the flowchart of Fig. 7. Assume that the customer applies for the mandatory automobile liability insurance, and upon complete application, the payment of the insurance money is confirmed (the withdrawal is confirmed in the case where the credit card is used). An instruction to issue the certificate is sent to the IC card reader/writer 200'. The IC card reader/writer 200', upon receipt of the instruction to issue the certificate, is supplied with the IC card, and the identification information reading means 26 reads the identification information 32 stored in advance in the IC card reader/writer 200' from the IC card 31 (S100). The identification information 32 thus read is transmitted by the identification information transmission means 27 from the communication unit 23 to the certificate management server 4 (S101).

[0056] The operation of the certificate management server 4

is similar to that explained in steps S200 to S205 of the embodiment described above and therefore not described in detail.

[0057] In the terminal 2, the authenticity receiving means 28 receives the authenticity information 33 indicating whether the identification information 32 transmitted from the certificate management server 4 is legitimate or not (S102), and in the case where the authenticity information 33 is genuine (S103), and the certificate issuance means 29 issues the IC card 31 as a certificate by additionally writing the contents of the certificate therein through the card reader/writer 200' (S104). In the case where the authenticity information 33 is false (S103), on the other hand, an error is displayed (S106).

[0058] Further, at the end of printing the certificate, the fact that the certificate has been issued is transmitted to the certificate management server 4 (S105). The certificate management server 4 receives the notice that the certificate has been issued (S206), so that the corresponding identification information 32 stored in the identification information database 41 is set as already issued (S207).

[0059] As explained in detail above, according to the second embodiment, the certificate can be issued in the form of the recording medium such as the IC card.

[0060] Next, according to a third embodiment, a case is explained in which the identification information is managed and the certificate is issued at each terminal (certificate issuance apparatus). The certificate issuance apparatus, as

explained with reference to Fig. 3, is installed inside the counter 7 of a convenience store or the like shop and includes the computer 203 such as a personal computer having the printing unit 200 such as a printer or, as shown in Fig. 5, the printing unit 200 such as a printer installed inside the counter 7 of a convenience store. Also, the apparatus may be a multi-function information terminal arranged in a shop like a convenience store.

[0061] The paper 3 with the built-in IC chip 31 is set by the insurance company in the certificate issuance apparatus installed in a shop. The identification information 32 of the IC chip 31 embedded in the paper 3 thus set is registered in a storage unit such as a hard disk having a certificate issuance apparatus by a portable medium such as FD (floppy (registered trade mark) disk) or CD-ROM.

[0062] The function of a certificate issuance apparatus 2' is explained with reference to the block diagram of Fig. 12. The certificate issuance apparatus 2' includes an identification information reader 26 constituting the identification information reader 204 for reading the identification information 32 stored in the recording medium 31 such as an IC chip, an authenticity confirmation means 28' for confirming the legitimacy of the identification information 32, a certificate issuance means 29 for issuing the certificate using a certificate issuance unit 25, and an identification information database 41' for registering the identification information 32 from the portable medium such as FD (floppy disk) or CD-ROM.

[0063] Next, with reference to the flowchart of Fig. 13, an explanation is given about the operation of the certificate issuance apparatus 2' installed inside the counter 7 of a shop like a convenience store and having the printing unit 200 such as a printer with the computer 203 such as a personal computer to issue a certificate. Further, the description that follows represents a case in which the certificate is issued on the paper with a built-in noncontact-type IC chip.

[0064] Assuming that the customer applies for the mandatory automobile liability insurance and the complete payment of the insurance money (the withdrawal in the case that the credit card is used) is confirmed, an instruction to issue a certificate is sent from the computer 203 to the printing unit 200. The printing unit 200, upon receipt of the instruction to issue the certificate, is supplied with the paper 3 with the built-in IC chip, and the identification information reading means 26 instructs the IC card reader (identification information reading unit) 204 to read the identification information 32 from the IC chip. The identification information 32 is transmitted from the IC chip and received by the IC card reader 204 (S300).

[0065] The authenticity confirmation means 28' judges whether the paper of the identification information 32 is legitimate or not. The identification information 32, if encrypted, is decrypted to judge whether the identification information 32 is legitimate or not (S301). In the case where the authenticity information 33 is genuine (S302), the certificate issuance means 29 prints the certificate using the printing unit 200 by

printing the contents of the certificate on the paper 3 with the built-in IC chip to issue the certificate (S303). In the case where the authenticity information 33 is false (S302), on the other hand, an error is displayed (S304).

[0066] For printing the certificate on the paper 3 with the built-in IC chip, the printing unit may include an IC card writer to write the required information in the IC chip.

[0067] The magnetic card (magnetic portion) instead of the IC chip may also be used. Further, in using a magnetic card, the identification information reader 204 is configured of a magnetic card reader/writer.

[0068] Furthermore, paper or the like printing material may be used with the identification information 32 printed thereon as a bar-code or a hologram, in which case the identification information reader 204 constitutes a bar-code reader or a hologram reader.

[0069] A case is explained above in which the identification information is registered in the database from a portable medium such as FD (floppy disk) or CD-ROM. Nevertheless, the portable medium such as FD (floppy disk) or CD-ROM may alternatively be installed in the certificate issuance apparatus to read the identification information directly.

[0070] As explained above, according to the third embodiment, even the apparatus not connected to a network can print the certificate such as the insurance policy of the mandatory automobile liability insurance by registering the identification information and judging whether the paper

distributed from the insurance company is legitimate or not.

[0071] As explained in the second embodiment, the recording medium 31 may also be issued as a certificate by the certificate issuance apparatus 2'. In this case, the certificate issuance means 29 additionally writes the contents of the certificate in the recording medium 31 such as the IC card by the recording medium writer such as the IC card writer to issue the IC card as a certificate.

[0072] A fourth embodiment is explained with reference to a case in which the certificate is issued by the multi-function information terminal installed in a shop such as a convenience store. In this embodiment, the same component parts as those of the embodiments described above are designated by the same reference numerals, respectively, and not described in detail. This embodiment has a similar configuration to the first embodiment shown in Fig. 1. Also, the terminal 2, different from the terminal 2 shown in Fig. 3, is a multi-function information terminal 2" installed in a convenience store or the like shop and including the identification information reader 204 for reading the identification information 32 stored in the recording medium 31 such as the IC chip attached to the printing material 3 as shown in Fig. 14 and the printing section 201 for printing the certificate. The multi-function information terminal 2" has the multiple types of functions including the issue of a ticket.

[0073] The functions of the multi-function information terminal 2" are similar to those of the terminal 2 of the

embodiments described above. Also, the operation of the certificate issuance system 1 is similar to that of the embodiments described above and therefore not described in detail.

[0074] Also, the certificate may be issued as the recording medium 31 such as the IC card.

[0075] As explained above, the certificate of the mandatory automobile liability insurance or the like can be printed upon judgment, by the multi-function information terminal installed in a shop such as a convenience store, whether the paper distributed from the insurance company is legitimate or not.

[0076]

[Effects of the Invention] As described above, according to the present invention, an illegal certificate can be prevented from being issued at a shop or an agent, thereby saving the illegal payment.

[0077] Also, the labor of collecting the recording medium such as blank paper distributed but not used or the wasteful disposal of the recording medium such as the paper left unused can be avoided.

[0078] Further, by reading the information stored in a recording medium and confirming the stored information by accessing the insurance company, the legitimate issue of the certificate can be confirmed.

[0079] Furthermore, the contents of the certificate can be issued in the recording medium.

[Brief Description of the Drawings]

[Fig. 1] A diagram showing the configuration of a certificate issuance system.

[Fig. 2] A diagram showing a recording medium attached to a printing material.

[Fig. 3] A diagram showing that a computer and a certificate management server are connected to each other through a network.

[Fig. 4] A diagram showing the mechanism of a printing unit.

[Fig. 5] A diagram showing that the printing unit and the certificate management server are connected to each other through a network.

[Fig. 6] A block diagram showing the functions of the certificate issuance system.

[Fig. 7] A flowchart showing the operation of the certificate issuance system

[Fig. 8] A diagram showing a configuration of the certificate issuance system according to a second embodiment.

[Fig. 9] A diagram showing that the computer and the certificate management server are connected to each other through a network.

[Fig. 10] A block diagram showing the function of the certificate issuance system according to the second embodiment.

[Fig. 11] A diagram showing the configuration of an IC card.

[Fig. 12] A block diagram showing the function of a certificate issuance apparatus.

[Fig. 13] A flowchart showing the operation of the certificate issuance apparatus.

[Fig. 14] A diagram showing the mechanism of a multi-function

information terminal.

[Description of Reference Numerals]

- 1 Certificate issuance system
- 2 Terminal
- 2' Certificate issuance apparatus
- 2" Multi-function information terminal
- 3 Recording medium
- 4 Certificate management server
- 5 Network
- 7 Inside shop counter
- 20 Bus line
- 21 Central processing unit (CPU)
- 22 Memory
- 23 Communication unit
- 26 Identification information reading means
- 27 Identification information transmission means
- 28 Authenticity receiving means
- 28' Authenticity confirmation means
- 29 Certificate issuance means
- 31 Recording medium
- 32 Identification information
- 33 Authenticity information
- 41, 41' Identification information database
- 42 Identification information receiving means
- 43 Authenticity judging means
- 44 Authenticity transmission means
- 200 Printing unit

200' Recording medium reader/writer
201 Printing section
202 Communication unit
203 Computer
204 Identification information reader
311 IC module
312 Terminal
313 IC chip

Fig. 7

CERTIFICATE MANAGEMENT SERVER
TERMINAL

S100 READ IDENTIFICATION INFORMATION
S101 TRANSMIT IDENTIFICATION INFORMATION
S200 RECEIVE IDENTIFICATION INFORMATION
S201 RETRIEVE IDENTIFICATION INFORMATION FROM IDENTIFICATION
INFORMATION DATABASE
S202 IDENTIFICATION INFORMATION OK?
S204 SET AUTHENTICITY INFORMATION AS FALSE
S203 SET AUTHENTICITY INFORMATION AS GENUINE
S205 TRANSMIT AUTHENTICITY INFORMATION
S102 RECEIVE AUTHENTICITY INFORMATION
S103 AUTHENTICITY INFORMATION GENUINE?
S104 ISSUE CERTIFICATE
S106 DISPLAY ERROR
S105 TRANSMIT NOTICE THAT CERTIFICATE HAS BEEN ISSUED
S206 RECEIVE NOTICE THAT CERTIFICATE HAS BEEN ISSUED
S207 CORRESPONDING IDENTIFICATION INFORMATION ALREADY ISSUED

FIG. 13

TERMINAL

S300 READ IDENTIFICATION INFORMATION
S301 CONFIRM WHETHER IDENTIFICATION INFORMATION IS GENUINE OR
FALSE
S302 AUTHENTICITY INFORMATION GENUINE?
S303 ISSUE CERTIFICATE

S304 DISPLAY ERROR

[Scope of Claim for a Patent]

[Claim 1] A certificate issuance system comprising at least a terminal installed in an agent of an insurance company or a shop such as a convenience store and a certificate management server connected to the terminal through a network for managing a printing material which is set in advance in the terminal exclusively to the insurance company and which carries an IC chip having recorded therein the identification information of the insurance company:

wherein the terminal includes an identification information reading means for reading the identification information, and an identification information transmission means for transmitting the identification information to the certificate management server;

wherein the certificate management server includes an identification information database for managing the identification information, and an authenticity transmission means for transmitting to the terminal authenticity information indicating whether the printing material is exclusive to the insurance company, based on the identification information; and

wherein the terminal includes a certificate issuance means for issuing a certificate of the insurance company by printing the contents of the certificate of the insurance company on the printing material exclusive to the insurance company.

[Claim 2] The certificate issuance system as set forth in claim 1, characterized in that the certificate issuance means stores

the contents of the certificate of the insurance company in the IC chip.

[Claim 3] A certificate issuance system comprising at least a terminal installed in an agent of an insurance company or a shop such as a convenience store and a certificate management server connected to the terminal through a network for managing a printing material which is set in advance in the terminal exclusively to the insurance company and which carries an IC chip having recorded therein the identification information of the insurance company; and

wherein the terminal includes:

an identification information reading means for reading the identification information;

an identification information transmission means for transmitting the identification information to the certificate management server;

an authenticity receiving means for receiving, from the certificate management server, authenticity information indicating whether the printing material is exclusive to the insurance company; and

a certificate issuance means for judging that the identification information is legitimate and issuing a certificate of the insurance company by printing the contents of the certificate of the insurance company on the printing material exclusive to the insurance company in the case where the authenticity information is genuine.

[Claim 4] A certificate issuance system comprising at least

a terminal installed in an agent of an insurance company or a shop such as a convenience store and a certificate management server connected to the terminal through a network for managing a printing material which is set in advance in the terminal exclusively to the insurance company and which carries an IC chip having recorded therein the identification information of the insurance company;

wherein the certificate management server includes:

an identification information receiving means for receiving the identification information from the terminal;

an identification information database for managing the identification information;

an authenticity judging means for retrieving the identification information from the identification information database and judging the authenticity as to whether the printing material is exclusive to the insurance company or not; and

an authenticity transmission means for transmitting authenticity information to the terminal to allow the terminal to issue a certificate of the insurance company on the printing material exclusive to the insurance company in the case where the authenticity information is genuine.

[Claim 5] A certificate issuance system comprising at least a terminal installed in an agent of an insurance company or a shop such as a convenience store and a certificate management server connected to the terminal through a network for managing a printing material which is set in advance in the terminal

exclusively to the insurance company and which carries an IC chip having recorded therein the identification information of the insurance company;

wherein the terminal includes an identification information reading means for reading the identification information and an identification information transmission means for transmitting the identification information to the certificate management server;

wherein the certificate management server includes an identification information database for managing the identification information and an authenticity transmission means for transmitting authenticity information indicating whether the IC card is exclusive to the insurance company or not to the terminal, based on the identification information; and

wherein the terminal includes a certificate issuance means for issuing the certificate of the insurance company by recording the contents of the certificate of the insurance company in the IC card exclusive to the insurance company in the case where the authenticity information is genuine.

[Claim 6] A certificate issuance system comprising at least a terminal installed in an agent of an insurance company or a shop such as a convenience store and a certificate management server connected to the terminal through a network for managing a printing material which is set in advance in the terminal exclusively to the insurance company and which carries an IC chip having recorded therein the identification information of

the insurance company;

wherein the terminal includes:

an identification information reading means for reading the identification information;

an identification information transmission means for transmitting the identification information to the certificate management server;

an authenticity receiving means for receiving from the certificate management server authenticity information indicating whether the IC card is that of the insurance company; and

a certificate issuance means for issuing a certificate of the insurance company by recording the contents of the certificate of the insurance company in the IC card exclusive to the insurance company in the case where the authenticity information is genuine.

[Claim 7] A certificate issuance system comprising at least a terminal installed in an agent of an insurance company or a shop such as a convenience store and a certificate management server connected to the terminal through a network for managing a printing material which is set in advance in the terminal exclusively to the insurance company and which carries an IC chip having recorded therein the identification information of the insurance company;

wherein the certificate management server includes:

an identification information receiving means for receiving the identification information from the terminal;

an identification information database for managing the identification information;

an authenticity judging means for retrieving identification information from the identification information database and judging the authenticity as to whether the IC card is exclusive to the insurance company; and

an authenticity transmission means for transmitting the authenticity information to the terminal to allow the terminal to issue a certificate of the insurance company on the IC card exclusive to the insurance company in the case where the authenticity information is genuine.

[Claim 8] A certificate issuance apparatus installed in an agent of an insurance company or a shop such as a convenience store and having preset therein a printing material exclusive to the insurance company carrying an IC chip for recording the identification information of the insurance company, comprising:

an identification information reading means for reading the identification information;

an identification information database for storing the identification information;

an authenticity judging means for judging the authenticity as to whether the identification information is that of the insurance company or not by searching the identification information database; and

a certificate issuance means for issuing a certificate of the insurance company by printing the contents of the

certificate of the insurance company on the printing material exclusive to the insurance company in the case where the authenticity information is genuine.

[Claim 9] A certificate issuance apparatus installed in an agent of an insurance company or a shop such as a convenience store and having preset therein an IC card exclusive to the insurance company for recording the identification information of the insurance company, comprising:

an identification information reading means for reading the identification information;

an identification information database for storing the identification information;

an authenticity judging means for judging the authenticity as to whether the identification information is legitimate or not by searching the identification information database; and

a certificate issuance means for issuing a certificate of the insurance company by recording the contents of the certificate of the insurance company on the IC card exclusive to the insurance company in the case where the authenticity information is genuine.

[Detailed Description of the Invention]

[0001]

[Technical Field of the Invention] The present invention relates to a certificate issuance system for issuing a certificate.

[0002]

[Prior Art] Conventionally, for mandatory automobile liability insurance or the like, a bundle of five vouchers handwritten by an agent or partly printed on a dot printer from an office computer is issued as a certificate. This certificate can be canceled whenever it become unrequired due to the scrapping or the like and a surrender value can be received with the cancellation.

[0003]

[Problem to be Solved by the Invention] Thus, an agent or the like can receive the surrender value by forging the vouchers illegally. In order to prevent the forgery, the vouchers are required to be kept under control. For example, the number of the vouchers deposited in an agent is managed and the vouchers are collected at intervals of several months by the insurance company. The sum of the number of applications for the mandatory automobile liability insurance filed by the agent and the number of the remaining vouchers is required to coincide with the initial number of vouchers deposited in the agent. Also, the vouchers miswritten, if any, by the agent are required to be kept in hand. This is not only a very bothersome job, but also the collection and the miswriting cause the wasteful disposal of about 30 to 40 % of the blank vouchers distributed from the insurance company.

[0004]

[Means for Solving the Problem] In order to solve the problem described above, according to claim 1 of the present invention, there is provided a certificate issuance system comprising at

least a terminal installed in an agent of an insurance company or a shop such as a convenience store and a certificate management server connected to the terminal through a network for managing a printing material which is set in advance in the terminal exclusively to the insurance company and which carries an IC chip having recorded therein the identification information of the insurance company: wherein the terminal includes an identification information reading means for reading the identification information, and an identification information transmission means for transmitting the identification information to the certificate management server; wherein the certificate management server includes an identification information database for managing the identification information, and an authenticity transmission means for transmitting to the terminal authenticity information indicating whether the printing material is exclusive to the insurance company, based on the identification information; and wherein the terminal includes a certificate issuance means for issuing a certificate of the insurance company by printing the contents of the certificate of the insurance company on the printing material exclusive to the insurance company in the case where the authenticity information is genuine.

[0005] In the configuration described above, the terminal has preset therein a printing material such as printable paper with a built-in IC chip exclusive to an insurance company with the identification information thereof recorded in the IC chip, and this terminal and the certificate management server for

managing the identification information recorded in the IC chip are connected to each other through a network, the terminal reads the identification information stored in the IC chip to issue the certificate, the identification information is transmitted to the certificate management server which confirms whether the printing material is exclusive to the insurance company or not, and in the case where the printing material is so exclusive, the terminal issues the certificate by printing the contents of the certificate of the insurance company on the printing material. The certificate is an insurance policy or the like document.

[0006] According to claim 2, there is provided the certificate issuance system as set forth in claim 1, characterized in that the certificate issuance means stores the contents of the certificate of the insurance company in the IC chip.

[0007] In the configuration described above, not only the certificate can be printed but also the contents of the certificate of the insurance company can be recorded in the IC chip as required .

[0008] According to claim 3, there is provided a certificate issuance system comprising at least a terminal installed in an agent of an insurance company or a shop such as a convenience store and a certificate management server connected to the terminal through a network for managing a printing material which is set in advance in the terminal exclusively to the insurance company and which carries an IC chip having recorded therein the identification information of the insurance

company; and wherein the terminal includes an identification information reading means for reading the identification information, an identification information transmission means for transmitting the identification information to the certificate management server, an authenticity receiving means for receiving, from the certificate management server, the authenticity information indicating whether the printing material is exclusive to the insurance company, and a certificate issuance means for judging that the identification information is legitimate and issuing a certificate of the insurance company by printing the contents of the certificate of the insurance company on the printing material exclusive to the insurance company in the case where the authenticity information is genuine.

[0009] In the configuration described above, the IC chip attached to the printing material such as paper for issuing the certificate of the insurance company has stored therein the identification information of the insurance company, the terminal has preset therein the printing material exclusive to the insurance company, the identification information of the printing material set at the terminal is read, the certificate management server confirms, based on the identification information whether the printing material is exclusive to the insurance company or not, and in the case where the printing material is so exclusive, the terminal issues the certificate of the insurance company by printing the contents of the certificate on the printing material such as paper.

[0010] According to claim 4, there is provided a certificate issuance system comprising at least a terminal installed in an agent of an insurance company or a shop such as a convenience store and a certificate management server connected to the terminal through a network for managing a printing material which is set in advance in the terminal exclusively to the insurance company and which carries an IC chip having recorded therein the identification information of the insurance company; wherein the certificate management server includes an identification information receiving means for receiving the identification information from the terminal, an identification information database for managing the identification information, an authenticity judging means for retrieving the identification information from the identification information database and judging the authenticity as to whether the printing material is exclusive to the insurance company or not, and an authenticity transmission means for transmitting authenticity information to the terminal to allow the terminal to issue a certificate of the insurance company on the printing material exclusive to the insurance company in the case where the authenticity information is genuine.

[0011] In the configuration described above, the certificate management server searches the identification information database according to the received identification information thereby to confirm, based on the identification information of the IC chip attached to the printing material such as paper

whether the printing material is exclusive to the insurance company or not, and in the case where the identification information is exclusive to the insurance company, the authenticity information is transmitted to the terminal to allow the terminal to print the contents of the certificate of the insurance company on the printing material.

[0012] According to claim 5, there is provided a certificate issuance system comprising at least a terminal installed in an agent of an insurance company or a shop such as a convenience store and a certificate management server connected to the terminal through a network for managing a printing material which is set in advance in the terminal exclusively to the insurance company and which carries an IC chip having recorded therein the identification information of the insurance company; wherein the terminal includes an identification information reading means for reading the identification information and an identification information transmission means for transmitting the identification information to the certificate management server; wherein the certificate management server includes an identification information database for managing the identification information and an authenticity transmission means for transmitting the authenticity information indicating whether the IC card is exclusive to the insurance company or not to the terminal, based on the identification information; and wherein the terminal includes a certificate issuance means for issuing a certificate of the insurance company by recording the contents of the

certificate of the insurance company in the IC card exclusive to the insurance company in the case where the authenticity information is genuine.

[0013] In the configuration described above, the terminal having preset therein the IC card exclusive to the insurance company with the identification information of the insurance company recorded therein and a certificate management server for managing the IC card are connected to each other through a network, the terminal reads the identification information stored in the IC card to issue the certificate of the insurance company, the identification information is transmitted to the certificate management server so that the certificate management server confirms whether the IC card is exclusive to the insurance company or not, and in the case where the IC card is so exclusive, the terminal issues the certificate by recording the contents of the certificate of the insurance company on the IC card.

[0014] According to claim 6, there is provided a certificate issuance system comprising at least a terminal installed in an agent of an insurance company or a shop such as a convenience store and a certificate management server connected to the terminal through a network for managing a printing material which is set in advance in the terminal exclusively to the insurance company and which carries an IC chip having recorded therein the identification information of the insurance company; wherein the terminal includes an identification information reading means for reading the identification

information, an identification information transmission means for transmitting the identification information to the certificate management server, an authenticity receiving means for receiving from the certificate management server the authenticity information indicating whether the IC card is that of the insurance company, and a certificate issuance means for issuing a certificate of the insurance company by recording the contents of the certificate of the insurance company in the IC card exclusive to the insurance company in the case where the authenticity information is genuine.

[0015] In the configuration described above, the IC card exclusive to the insurance company having recorded therein the identification information of the insurance company is preset at the terminal, which reads the identification information stored in the IC card so that the certificate management server confirms whether the IC card is exclusive to the insurance company or not, and in the case where the IC card is so exclusive, the terminal issues the certificate by recording the contents of the certificate of the insurance company on the IC card.

[0016] According to claim 7, there is provided a certificate issuance system comprising at least a terminal installed in an agent of an insurance company or a shop such as a convenience store and a certificate management server connected to the terminal through a network for managing a printing material which is set in advance in the terminal exclusively to the insurance company and which carries an IC chip having recorded therein the identification information of the insurance

company; wherein the certificate management server includes an identification information receiving means for receiving the identification information from the terminal, an identification information database for managing the identification information, an authenticity judging means for retrieving the identification information from the identification information database and judging the authenticity as to whether the IC card is exclusive to the insurance company, and an authenticity transmission means for transmitting the authenticity information to the terminal to allow the terminal to issue the certificate of the insurance company on the IC card exclusive to the insurance company in the case where the authenticity information is genuine.

[0017] In the configuration described above, the certificate management server, by searching the identification information database according to the received identification information, confirms whether the IC card is exclusive to the insurance company or not, and in the case where the IC card is so exclusive, the authenticity information is transmitted to the terminal so that the terminal may record the contents of the certificate of the insurance company on the IC card.

[0018] According to claim 8, there is provided a certificate issuance apparatus installed in an agent of an insurance company or a shop such as a convenience store and having preset therein a printing material with a built-in IC chip exclusive to the insurance company for recording the identification information of the insurance company, comprising: an identification

information reading means for reading the identification information; an identification information database for storing the identification information; an authenticity judging means for judging the authenticity as to whether the identification information is legitimate or not by searching the identification information database; and a certificate issuance means for issuing the certificate of the insurance company by printing the contents of the certificate of the insurance company on the printing material exclusive to the insurance company in the case where the authenticity information is genuine.

[0019] In the configuration described above, the identification information of the insurance company is stored in the IC chip attached to the printing material such as paper, the printing material is preset, the identification information of the IC chip is read thereby to confirm based on the identification information whether the printing material is exclusive to the insurance company or not, and in the case where the printing material is so exclusive, the certificate is issued by printing the contents of the certificate of the insurance company on the printing material.

[0020] According to claim 9, there is provided a certificate issuance apparatus installed in an agent of an insurance company or a shop such as a convenience store and having preset therein an IC card exclusive to the insurance company for recording the identification information of the insurance company, comprising: an identification information reading means for

reading the identification information; an identification information database for storing the identification information; an authenticity judging means for judging the authenticity by searching the identification information database as to whether the identification information is legitimate or not; and a certificate issuance means for issuing the certificate of the insurance company by recording the contents of the certificate of the insurance company on the IC card exclusive to the insurance company in the case where the authenticity information is genuine.

[0021] In the configuration described above, the IC card exclusive to the insurance company having recorded therein the identification information of the insurance company is preset, the identification information of the IC card is read thereby to confirm based on the identification information whether the IC card is exclusive to the insurance company or not, and in the case where the IC card is so exclusive, the certificate is issued by storing the contents of the certificate of the insurance company.

[0022]

[Mode for Carrying out the Invention] Embodiments of the present invention are described below with reference to the drawings. Fig. 1 is a diagram showing the configuration of a certificate issuance system 1 of the invention. The certificate issuance system 1 includes a terminal 2 for issuing a certificate by printing the certificate on a printing material 3 having attached thereto a recording medium 31 prepared in

advance, a certificate management server 4 for managing the recording medium and a network 5. The identification information is stored in the recording medium 31, and the certificate management server 4 has an identification information database 41 for managing the identification information. This embodiment is described below with reference to a case in which the terminal 2 is installed in a shop such as a convenience store or an agent to issue the insurance policy for the mandatory automobile liability insurance or the like. Also, the printing material 3 with the recording medium 31 attached thereto is distributed to the shop such as the convenience store or the agent from an organization issuing the certificate on behalf of an insurance company.

[0023] The printing material 3 with the recording medium 31 attached thereto, as an example thereof shown in Fig. 2, is typically paper to which the recording medium 31 such as an IC chip, a magnetic card (magnetic portion), a bar-code or a hologram is attached. Specifically, it is the paper with a built-in semiconductor such as an IC chip, the paper with a magnetic card (magnetic portion) attached thereto or the paper printed with a bar-code or a hologram. The IC chip, configured of a CPU and a memory, has the function as a computer. Also, the IC chip has an antenna capable of input/output without contact, or has an IC chip with a terminal for input/output by contact.

[0024] The identification information is uniquely assigned by the insurance company or the like organization issuing the

certificate and formed of a randomly assigned number or an encrypted data. Also, the identification information is stored in the magnetic portion of the magnetic card or the semiconductor such as the IC chip (contact or noncontact type). As an alternative, it is contained as information in a bar-code or a hologram. The data is preferably stored in the semiconductor such as the IC chip not in a rewritable way.

[0025] The terminal 2 is, as shown in Fig. 3, for example, is arranged inside a counter 7 of a shop such as a convenience store and so configured that a printing unit 200 such as a printer with an identification information reader 204 is connected to a computer 203 such as a personal computer so that the data is transmitted to or received from the certificate management server 4 using the communication function of the computer 203. Also, the printing unit 200, as shown in Fig. 4, includes a printing section 201, the identification information reader 204 and a communication unit 202 connected to the computer 203.

[0026] The identification information reader 204 is a unit such as an IC card reader (including the means for reading the IC chip) for reading the identification information stored in the various recording media 3.

[0027] The identification information reader 204 is a unit such as an IC card reader (including the means for reading the IC chip), a magnetic data reader, a hologram reader or the bar-code reader for reading the identification information stored in the various recording media 3.

[0028] The terminal 2, as shown in Fig. 5, may be so configured

that the printing unit 200 such as a printer is arranged inside the counter 7 of a shop like a convenience store and the communication unit 202 has the function of transmitting and receiving data to and from the certificate management server 4.

[0029] As an alternative, the certificate may be issued by a multi-function information terminal which may be installed in a convenience store or the like.

[0030] The certificate management server 4 is a computer having a central processing unit such as a CPU, a memory such as a RAM or a ROM and a communication unit. Further, the certificate management server 4 includes an identification information database 41 for managing identification information 32 of the recording medium 31. The communication unit has the function of transmitting and receiving the data to and from the network 5.

[0031] The network 5 connecting the terminal 2 and the certificate management server 4 can take any of various channel forms including a dedicated line, a public line such as ISDN and radio communication. Further, the internet may be used in the configuration. To secure the reliability of information management, however, a network having a high security is desired.

[0032] Next, the function of the certificate issuance system 1 is explained with reference to the block diagram of Fig. 6. The terminal 2 includes an identification information reading means 26 having the identification information reader 204 for

reading the identification information 32 stored in the recording medium 31 such as an IC chip, an identification information transmission means 27 for transmitting the identification information 32 to the certificate management server 4, an authenticity receiving means 28 for receiving, from the certificate management server 4, authenticity information 33 indicating whether the identification information 32 is legitimate or not, and a certificate issuance means 29 for issuing a certificate using the printing unit 200.

[0033] The certificate management server 4 includes the identification information database 41 for managing the identification information 32 of the recording medium 3 distributed, an identification information receiving means 42 for receiving the identification information 32 from the terminal 2, an authenticity judging means 43 for judging the authenticity of the identification information by searching the identification information database 41 to check whether the identification information 32 is in the identification information database 41 or not, and an authenticity transmission means 44 for transmitting the authenticity information indicating the authenticity to the terminal 2. The authenticity judging means 43 may also be configured to execute the decryption process in the case where the identification information is encrypted.

[0034] Next, the operation of the certificate issuance system 1 is explained with reference to the flowchart shown in Fig. 7. A case is taken up in which an insurance company issues a

certificate of the mandatory automobile liability insurance or the like using the paper (printing material) 3 with a built-in IC chip (recording medium 31). In the case, the terminal 2 is installed inside the counter 7 of a shop such as a convenience store and issues the certificate using the printing unit 200 such as a printer from the computer 203 such as a personal computer. Further, in this case, the noncontact-type IC chip is used as the recording medium 31, and the IC card reader as the identification information reader 204.

[0035] First, the paper 3 with the built-in IC chip 31 is distributed from the insurance company to the shop such as a convenience store. The insurance company stores the identification information 32 in the IC chip 31 in advance. The paper 3 with the built-in IC chip 31 is set in the printing unit 200 installed inside the counter of the shop.

[0036] Assume that the customer applies for the mandatory automobile liability insurance and that upon completion of the application, the payment of the insurance money is confirmed (the withdrawal is confirmed in the case of the credit card is used). An instruction to issue a certificate is then sent from the computer 203 to the printing unit 200. The printing unit 200, upon receipt of the instruction to issue the certificate, is supplied with the paper 3 with the built-in IC chip 31, and an instruction to read the identification information 32 is transmitted to the IC chip 31 from the IC card reader (identification information reading unit) 204 of the identification information reading means 26. The

identification information 32 is sent from the IC chip 31 and received by the IC card reader 204 (S100). The identification information transmission means 27 transmits the received identification information 32 from the communication unit 23 to the certificate management server 4 (S101).

[0037] In the certificate management server 4, the identification information receiving means 42 receives the identification information 32 (S200), and the authenticity judging means 43 searches the identification information database for the identification information 32 (S201) and judges whether the identification information 32 is legitimate or not. The identification information 32, if encrypted, is decrypted and retrieved from the identification information database 41 (S201) thereby to judge whether the identification information 32 is legitimate or not. In the case where the identification information 32 is legitimate (S202), the authenticity information 33 is determined as genuine (S205), while in the case where the identification information 32 is not legitimate (S204), the authenticity information 33 is determined as false (S205). Further, the authenticity transmission means 44 transmits the authenticity information 33 to the terminal 2.

[0038] The authenticity receiving means 28 of the terminal 2 receives the authenticity information 33 through the communication unit 23 (S102), and in the case where the authenticity information 33 is genuine (S103), the certificate issuance means 29 issues the certificate by printing the

contents of the certificate on the paper 3 with the built-in IC chip using the printing unit 200 (S104). In the case where the authenticity information 33 is false (S103), on the other hand, an error is displayed (S106).

[0039] Further, at the end of printing the certificate, the fact that the certificate is issued is transmitted to the certificate management server 4 (S105). The certificate management server 4 receives the notice that the certificate is already issued (S206) and the identification information 32 stored in the identification information database 41 is set as issued (S207).

[0040] In printing the certificate on the paper 3 with the built-in IC chip 31, the IC card writer may be provided on the printing unit to write the required information in the IC chip 31.

[0041] As explained above, the certificate of the mandatory automobile liability insurance or the like can be printed only on the paper distributed from the insurance company based on the identification information 32.

[0042] Also, at the time of paying the insurance money or the surrender value due to the scrapping according to the mandatory automobile liability insurance, the information (including the identification information) stored in the IC chip may be read to confirm that the certificate is legitimate.

[0043] The noncontact-type IC chip explained above may be replaced with the contact-type IC chip. In that case, the IC chip reader/writer is configured in such a manner that the

position for reading/writing the IC chip can be fixed. As an alternative, also at the time of using the magnetic card, the magnetic card reader/writer is configured in such a manner that the position of reading/writing the magnetic card can be fixed.

[0044] Further, the paper or the like printing material with the identification information 32 printed as a bar-code or a hologram thereon may be used, in which case the identification information reader 204 is a bar-code reader or a hologram reader.

[0045] As explained in detail above, according to the first embodiment, the identification information attached to the printing material such as paper is confirmed, and by thus judging whether the identification information is a legitimate one distributed from the insurance company, the certificate of the mandatory automobile liability insurance or the like can be printed.

[0046] Next, according to a second embodiment, an explanation is given about a case in which the certificate is issued by the recording medium 31. The same component parts as those in the aforementioned embodiment are designated by the same reference numerals, respectively, and not described in detail any further. Fig. 8 shows the configuration of the certificate issuance system 1 according to the second embodiment. In the second embodiment, the terminal 2 issues the certificate is issued in the form of the recording medium 31 such as an IC card with a built-in IC chip.

[0047] The terminal 2 is configured, as an example, in such

a manner that as shown in Fig. 9, the computer 203 such as the personal computer is connected with a recording medium reader/writer 200' such as an IC card reader/writer, and by utilizing the communication function of the computer 203, the data is transmitted to and received from the certificate management server 4.

[0048] According to the second embodiment, the function of the certificate issuance system 1 is explained with reference to the block diagram of Fig. 10. In the identification information reader 26 of the terminal 2, the recording medium reader/writer 200' such as the IC card reader/writer reads the identification information 32 stored in the recording medium 31 such as an IC card, and the certificate issuance means 29 issues the certificate using the recording medium reader/writer 200' such as the IC card reader/writer.

[0049] The recording medium 31 may be a plastic card with a built-in IC chip, a magnetic card with the magnetic tape attached to a plastic card, an optical disk such as CD-ROM, CD-RW, or a magnetic medium such as MO, MD or FD. This recording medium 31 is uniquely assigned the identification information 32 by an organization such as an insurance company issuing the certificate, and the contents of the certificate are additionally written in the recording medium 31 and then issued as a certificate.

[0050] The description that follows represents a case in which the IC card (recording medium) 31 is issued as a certificate. The IC card 31, as shown in Fig. 11, is formed of a plastic card

with a built-in IC module 311. The IC module 311 is configured of an IC chip 313 having a terminal 312 for data input/output. The IC card reader inputs/outputs the data after being brought into contact with the terminal 312 or without contact with the terminal 312 acting as an antenna.

[0051] The operation of the certificate issuance system 1 different from the operation of the aforementioned embodiment is explained with the flowchart of Fig. 7. Assume that the customer applies for the mandatory automobile liability insurance, and upon complete application, the payment of the insurance money is confirmed (the withdrawal is confirmed in the case where the credit card is used). An instruction to issue the certificate is sent to the IC card reader/writer 200'. The IC card reader/writer 200', upon receipt of the instruction to issue the certificate, is supplied with the IC card, and the identification information reading means 26 reads the identification information 32 stored in advance in the IC card reader/writer 200' from the IC card 31 (S100). The identification information 32 thus read is transmitted by the identification information transmission means 27 from the communication unit 23 to the certificate management server 4 (S101).

[0052] The operation of the certificate management server 4 is similar to that explained in steps S200 to S205 of the embodiment described above and therefore not described in detail.

[0053] In the terminal 2, the authenticity receiving means 28

receives the authenticity information 33 indicating whether the identification information 32 transmitted from the certificate management server 4 is legitimate or not (S102), and in the case where the authenticity information 33 is genuine (S103), and the certificate issuance means 29 issues the IC card 31 as a certificate by additionally writing the contents of the certificate therein through the card reader/writer 200' (S104). In the case where the authenticity information 33 is false (S103), on the other hand, an error is displayed (S106).

[0054] Further, at the end of printing the certificate, the fact that the certificate has been issued is transmitted to the certificate management server 4 (S105). The certificate management server 4 receives the notice that the certificate has been issued (S206), so that the corresponding identification information 32 stored in the identification information database 41 is set as already issued (S207).

[0055] As explained in detail above, according to the second embodiment, the certificate can be issued in the form of the recording medium such as the IC card.

[0056] Next, according to a third embodiment, a case is explained in which the identification information is managed and the certificate is issued at each terminal (certificate issuance apparatus). The certificate issuance apparatus, as explained with reference to Fig. 3, is installed inside the counter 7 of a convenience store or the like shop and includes the computer 203 such as a personal computer having the printing unit 200 such as a printer or, as shown in Fig. 5, the printing

unit 200 such as a printer installed inside the counter 7 of a convenience store. Also, the apparatus may be a multi-function information terminal arranged in a shop like a convenience store.

[0057] The paper 3 with the built-in IC chip 31 is set by the insurance company in the certificate issuance apparatus installed in a shop. The identification information 32 of the IC chip 31 embedded in the paper 3 thus set is registered in a storage unit such as a hard disk having a certificate issuance apparatus by a portable medium such as FD (floppy (registered trade mark) disk) or CD-ROM.

[0058] The function of a certificate issuance apparatus 2' is explained with reference to the block diagram of Fig. 12. The certificate issuance apparatus 2' includes an identification information reader 26 constituting the identification information reader 204 for reading the identification information 32 stored in the recording medium 31 such as an IC chip, an authenticity confirmation means 28' for confirming the legitimacy of the identification information 32, a certificate issuance means 29 for issuing the certificate using a certificate issuance unit 25, and an identification information database 41' for registering the identification information 32 from the portable medium such as FD (floppy disk) or CD-ROM.

[0059] Next, with reference to the flowchart of Fig. 13, an explanation is given about the operation of the certificate issuance apparatus 2' installed inside the counter 7 of a shop like a convenience store and having the printing unit 200 such

as a printer with the computer 203 such as a personal computer to issue a certificate. Further, the description that follows represents a case in which the certificate is issued on the paper with a built-in noncontact-type IC chip.

[0060] Assuming that the customer applies for the mandatory automobile liability insurance and the complete payment of the insurance money (the withdrawal in the case that the credit card is used) is confirmed, an instruction to issue a certificate is sent from the computer 203 to the printing unit 200. The printing unit 200, upon receipt of the instruction to issue the certificate, is supplied with the paper 3 with the built-in IC chip, and the identification information reading means 26 instructs the IC card reader (identification information reading unit) 204 to read the identification information 32 from the IC chip. The identification information 32 is transmitted from the IC chip and received by the IC card reader 204 (S300).

[0061] The authenticity confirmation means 28' judges whether the paper of the identification information 32 is legitimate or not. The identification information 32, if encrypted, is decrypted to judge whether the identification information 32 is legitimate or not (S301). In the case where the authenticity information 33 is genuine (S302), the certificate issuance means 29 prints the certificate using the printing unit 200 by printing the contents of the certificate on the paper 3 with the built-in IC chip to issue the certificate (S303). In the case where the authenticity information 33 is false (S302), on the other hand, an error is displayed (S304).

[0062] For printing the certificate on the paper 3 with the built-in IC chip, the printing unit may include an IC card writer to write the required information in the IC chip.

[0063] The magnetic card (magnetic portion) instead of the IC chip may also be used. Further, in using a magnetic card, the identification information reader 204 is configured of a magnetic card reader/writer.

[0064] Furthermore, paper or the like printing material may be used with the identification information 32 printed thereon as a bar-code or a hologram, in which case the identification information reader 204 constitutes a bar-code reader or a hologram reader.

[0065] A case is explained above in which the identification information is registered in the database from a portable medium such as FD (floppy disk) or CD-ROM. Nevertheless, the portable medium such as FD (floppy disk) or CD-ROM may alternatively be installed in the certificate issuance apparatus to read the identification information directly.

[0066] As explained above, according to the third embodiment, even the apparatus not connected to a network can print the certificate such as the insurance policy of the mandatory automobile liability insurance by registering the identification information and judging whether the paper distributed from the insurance company is legitimate or not.

[0067] As explained in the second embodiment, the recording medium 31 may also be issued as a certificate by the certificate issuance apparatus 2'. In this case, the certificate issuance

means 29 additionally writes the contents of the certificate in the recording medium 31 such as the IC card by the recording medium writer such as the IC card writer to issue the IC card as a certificate.

[0068] A fourth embodiment is explained with reference to a case in which the certificate is issued by the multi-function information terminal installed in a shop such as a convenience store. In this embodiment, the same component parts as those of the embodiments described above are designated by the same reference numerals, respectively, and not described in detail. This embodiment has a similar configuration to the first embodiment shown in Fig. 1. Also, the terminal 2, different from the terminal 2 shown in Fig. 3, is a multi-function information terminal 2" installed in a convenience store or the like shop and including the identification information reader 204 for reading the identification information 32 stored in the recording medium 31 such as the IC chip attached to the printing material 3 as shown in Fig. 14 and the printing section 201 for printing the certificate. The multi-function information terminal 2" has the multiple types of functions including the issue of a ticket.

[0069] The functions of the multi-function information terminal 2" are similar to those of the terminal 2 of the embodiments described above. Also, the operation of the certificate issuance system 1 is similar to that of the embodiments described above and therefore not described in detail.

[0070] Also, the certificate may be issued as the recording medium 31 such as the IC card.

[0071] As explained above, the certificate of the mandatory automobile liability insurance or the like can be printed upon judgment, by the multi-function information terminal installed in a shop such as a convenience store, whether the paper distributed from the insurance company is legitimate or not.

[0072]

[Effects of the Invention] As described above, according to the present invention, by setting a printing material or an IC card exclusive to an insurance company previously in a terminal installed in an agent of the insurance company or a shop such as a convenience store, an illegal certificate can be prevented from being issued at a shop or an agent, thereby saving the illegal payment.

[0073] Also, the labor of collecting the printing material or the IC card such as blank paper distributed but not used or the wasteful disposal of the printing material or the IC card such as the paper left unused can be avoided.

[0074] Further, by reading the information stored in a recording medium and confirming the stored information by accessing the insurance company, the legitimate issue of the certificate can be confirmed.

[0075] Furthermore, the contents of the certificate can be issued in the recording medium.

[Brief Description of the Drawings]

[Fig. 1] A diagram showing the configuration of a certificate

issuance system.

[Fig. 2] A diagram showing a recording medium attached to a printing material.

[Fig. 3] A diagram showing that a computer and a certificate management server are connected to each other through a network.

[Fig. 4] A diagram showing the mechanism of a printing unit.

[Fig. 5] A diagram showing that the printing unit and the certificate management server are connected to each other through a network.

[Fig. 6] A block diagram showing the functions of the certificate issuance system.

[Fig. 7] A flowchart showing the operation of the certificate issuance system

[Fig. 8] A diagram showing a configuration of the certificate issuance system according to a second embodiment.

[Fig. 9] A diagram showing that the computer and the certificate management server are connected to each other through a network.

[Fig. 10] A block diagram showing the function of the certificate issuance system according to the second embodiment.

[Fig. 11] A diagram showing the configuration of an IC card.

[Fig. 12] A block diagram showing the function of a certificate issuance apparatus.

[Fig. 13] A flowchart showing the operation of the certificate issuance apparatus.

[Fig. 14] A diagram showing the mechanism of a multi-function information terminal.

[Description of Reference Numerals]

1	Certificate issuance system
2	Terminal
2'	Certificate issuance apparatus
2"	Multi-function information terminal
3	Recording medium
4	Certificate management server
5	Network
7	Inside shop counter
20	Bus line
21	Central processing unit (CPU)
22	Memory
23	Communication unit
26	Identification information reading means
27	Identification information transmission means
28	Authenticity receiving means
28'	Authenticity confirmation means
29	Certificate issuance means
31	Recording medium
32	Identification information
33	Authenticity information
41, 41'	Identification information database
42	Identification information receiving means
43	Authenticity judging means
44	Authenticity transmission means
200	Printing unit
200'	Recording medium reader/writer

- 201 Printing section
- 202 Communication unit
- 203 Computer
- 204 Identification information reader
- 311 IC module
- 312 Terminal
- 313 IC chip

(19)日本国特許庁(JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-269271

(P2002-269271A)

(43)公開日 平成14年9月20日(2002.9.20)

(51)Int.Cl. ⁷	識別記号	F I	ターミナル*(参考)	
G 0 6 F 17/60	1 4 0	G 0 6 F 17/60	1 4 0	2 C 0 0 0
	1 5 4		1 5 4	5 B 0 3 0
	2 1 4		2 1 4	5 B 0 5 8
	2 3 4		2 3 4 C	
			2 3 4 E	

審査請求 有 請求項の数 9 O L (全 19 頁) 最終頁に続く

(21)出願番号 特願2001-69385(P2001-69385)

(22)出願日 平成13年3月12日(2001.3.12)

(71)出願人 592018320

あいおい損害保険株式会社

東京都渋谷区恵比寿一丁目28番1号

(72)発明者 佐藤 順一

東京都渋谷区代々木3丁目25番3号 大東

京火災海上保険株式会社内

(74)代理人 100081271

弁理士 吉田 芳春

Fターム(参考) 2C005 MA03 MB01 NA02 NA08 NB03

SA22

5B035 AA13 BB01 BB02 BB05 BB09

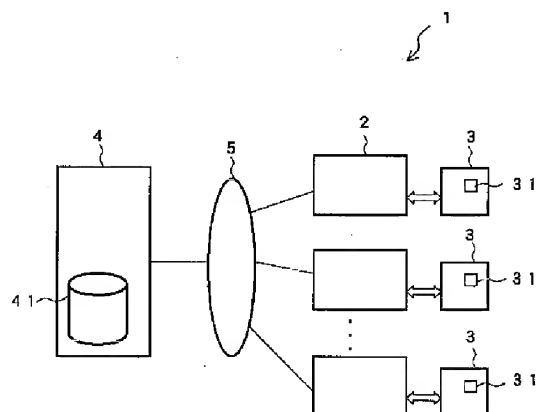
5B058 CA31 KA11 KA31

(54)【発明の名称】 証明書発行システムおよび証明書発行装置

(57)【要約】

【課題】 代理店などで帳票を不正に使用した証明書の偽造を防ぐ。

【解決手段】 証明書を発行するための紙などの印刷材料3を備える端末2と印刷材料3を管理する証明書管理サーバ4とがネットワーク5を介して接続し、端末2で、印刷材料3に付けられている識別情報31を読み取り、識別情報31を証明書管理サーバ4に送信し、識別情報31が正当なものであるかを確認して、端末2で、印刷材料31に証明書の内容を記録して証明書を発行する。



【特許請求の範囲】

【請求項1】 印刷素材に付した記録媒体の識別情報を読み取る端末と前記記録媒体を管理する証明書管理サーバとがネットワークを介して接続し、
前記端末は、
前記記録媒体の識別情報を読み取る識別情報読み取り手段と、
前記識別情報を前記証明書管理サーバに送信する識別情報送信手段とを備え、
前記証明書管理サーバは、
前記識別情報を管理する識別情報データベースと、
前記識別情報より前記記録媒体が正当であるか否かを表す真偽情報を前記端末に送信する真偽送信手段とを備え、
前記端末は、
前記真偽情報が真の場合には、前記印刷素材に証明書の内容を印刷して証明書を発行する証明書発行手段を備える証明書発行システム。

【請求項2】 請求項1記載の証明書発行システムにおいて、
前記記録媒体は、識別情報を記憶したICチップであることを特徴とする証明書発行システム。

【請求項3】 請求項1または2記載の証明書発行システムにおいて、
前記証明書発行手段で、記録媒体に証明書の内容を記憶することを特徴とする証明書発行システム。

【請求項4】 印刷素材に付した記録媒体の識別情報を読み取る端末と前記記録媒体を管理する証明書管理サーバとがネットワークを介して接続し、
前記端末は、
前記記録媒体の識別情報を読み取る識別情報読み取り手段と、
前記識別情報を前記証明書管理サーバに送信する識別情報送信手段と、
前記記録媒体が正当であるか否かを表す真偽情報を前記証明書管理サーバから受信する真偽受信手段と、
前記真偽情報が真の場合には、前記記録媒体が正当であると判断して前記印刷素材に証明書の内容を印刷して証明書を発行する証明書発行手段とを備える証明書発行システム。

【請求項5】 印刷素材に付した記録媒体の識別情報を読み取る端末と前記記録媒体を管理する証明書管理サーバとがネットワークを介して接続し、
前記証明書管理サーバは、
前記記録媒体の識別情報を前記端末から受信する識別情報受信手段と、
前記識別情報を管理する識別情報データベースと、
前記識別情報を前記識別情報データベースより検索して、正当であるか否かの真偽を判断する真偽判定手段と、

真偽を判定し真の場合には前記端末で証明書を発行する真偽情報を前記端末に送信する真偽送信手段とを備える証明書発行システム。

【請求項6】 記録媒体の識別情報を読み取る端末と前記記録媒体を管理する証明書管理サーバとがネットワークを介して接続し、
前記端末は、
前記記録媒体の識別情報を読み取る識別情報読み取り手段と、
前記識別情報を前記証明書管理サーバに送信する識別情報送信手段とを備え、
前記証明書管理サーバは、
前記識別情報を管理する識別情報データベースと、
前記識別情報より前記記録媒体が正当であるか否かを表す真偽情報を前記端末に送信する真偽送信手段とを備え、
前記端末は、
前記真偽情報が真の場合には、前記記録媒体に証明書の内容を記録して証明書を発行する証明書発行手段を備える証明書発行システム。

【請求項7】 請求項6記載の証明書発行システムにおいて、
前記記録媒体は、識別情報を記憶したICカードであることを特徴とする証明書発行システム。

【請求項8】 記録媒体の識別情報を読み取る端末と前記記録媒体を管理する証明書管理サーバとがネットワークを介して接続し、
前記端末は、
前記記録媒体の識別情報を読み取る識別情報読み取り手段と、
前記識別情報を前記証明書管理サーバに送信する識別情報送信手段と、
前記記録媒体が正当であるか否かを表す真偽情報を前記証明書管理サーバから受信する真偽受信手段と、
前記真偽情報が真の場合には、前記記録媒体が正当であると判断して前記記録媒体に証明書の内容を記録して証明書を発行する証明書発行手段とを備える証明書発行システム。

【請求項9】 記録媒体の識別情報を読み取る端末と前記記録媒体を管理する証明書管理サーバとがネットワークを介して接続し、
前記証明書管理サーバは、
前記記録媒体の識別情報を前記端末から受信する識別情報受信手段と、
前記識別情報を管理する識別情報データベースと、
前記識別情報を前記識別情報データベースより検索して、正当であるか否かの真偽を判断する真偽判定手段と、
真偽を判定し真の場合には前記端末で証明書を発行する真偽情報を前記端末に送信する真偽送信手段とを備える

証明書発行システム。

【請求項10】 印刷素材に付された記録媒体の識別情報を読み取る識別情報読み取り手段と、識別情報を格納する識別情報データベースを備え、前記識別情報が正当であるか否かを前記識別情報データベースで検索して真偽を判断する真偽判断手段と、前記真偽情報が真の場合には、印刷素材に証明書の内容を印刷して証明書を発行する証明書発行手段を備える証明書発行装置。

【請求項11】 記録媒体の識別情報を読み取る識別情報読み取り手段と、識別情報を格納する識別情報データベースを備え、前記識別情報が正当であるか否かを前記識別情報データベースで検索して真偽を判断する真偽判断手段と、前記真偽情報が真の場合には、記録媒体に証明書の内容を記録して証明書を発行する証明書発行手段を備える証明書発行装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、証明書を発行するための証明書発行システムに関する。

【0002】

【従来の技術】従来は、自賠責保険などは、代理店で手書き、或いは、一部オフコンからドットプリンターで5枚綴りの帳票に印刷したものを証明書としていた。この証明書は、廃車などにともない不要になると解約することができ、解約に伴い返還金を受け取ることができる。

【0003】

【発明が解決しようとする課題】そこで、代理店などでこの帳票を不正に使用して偽造し、この返還金を受け取ることが可能である。この偽造を防ぐために、常に、帳票の管理を行わなければ行けない。例えば、代理店に置く帳票の枚数を保険会社が管理し、数か月単位で回収して、その代理店から申し込まれた自賠責保険の件数と残っている帳票の数の合計が、始めに置いた帳票の枚数と一致しなければならない。また、代理店で書き損じ（書損）の帳票も必ず取っておく必要があり大変煩わしかった。さらに、この回収と書損に伴い、現在保険会社から白紙で配布された帳票の内約3〜4割が廃棄され無駄が多かった。

【0004】

【課題を解決するための手段】前述の課題を解決するため、本発明に係る証明書発行システムの、請求項1では、印刷素材に付した記録媒体の識別情報を読み取る端末と前記記録媒体を管理する証明書管理サーバとがネットワークを介して接続し、前記端末は、前記記録媒体の識別情報を読み取る識別情報読み取り手段と、前記識別情報を前記証明書管理サーバに送信する識別情報送信手段とを備え、前記証明書管理サーバは、前記識別情報を管理する識別情報データベースと、前記識別情報より前

記記録媒体が正当であるか否かを表す真偽情報を前記端末に送信する真偽送信手段とを備え、前記端末は、前記真偽情報が真の場合には、前記印刷素材に証明書の内容を印刷して証明書を発行する証明書発行手段を備える。

【0005】上記構成によれば、ICカードや磁気カードなどの記録媒体とその記録媒体であるICカードに含まれるICチップや磁気カードなどの磁気部分を付した紙など印刷可能な素材である印刷素材に証明書を発行する端末と、記録媒体に記録された識別情報を管理する証明書管理サーバがネットワークを介して接続され、端末で証明書を発行するために記録媒体に記憶された識別情報を読み取り、識別情報を証明書管理サーバに送信して、証明書管理サーバで記録媒体が正当であるか否かを確認し、正当な記録媒体であれば、端末で印刷素材に証明書の内容を印刷して証明書を発行する。証明書とは、保険証券類や戸籍謄本や住民票などを含む概念である。

【0006】また、請求項2では、請求項1記載の証明書発行システムにおいて、前記記録媒体は、識別情報を記憶したICチップであることを特徴とする。

【0007】上記構成によれば、記録媒体はICチップで、識別情報を記憶する事が可能である。

【0008】また、請求項3では、請求項1または2記載の証明書発行システムにおいて、前記証明書発行手段で、記録媒体に証明書の内容を記憶することを特徴とする。

【0009】上記構成によれば、証明書を印刷するだけでなく必要に応じて記録媒体に証明書の内容を記録することが可能である。

【0010】また、請求項4では、印刷素材に付した記録媒体の識別情報を読み取る端末と前記記録媒体を管理する証明書管理サーバとがネットワークを介して接続し、前記端末は、前記記録媒体の識別情報を読み取る識別情報読み取り手段と、前記識別情報を前記証明書管理サーバに送信する識別情報送信手段と、前記記録媒体が正当であるか否かを表す真偽情報を前記証明書管理サーバから受信する真偽受信手段と、前記真偽情報が真の場合には、前記記録媒体が正当であると判断して前記印刷素材に証明書の内容を印刷して証明書を発行する証明書発行手段とを備える。

【0011】上記構成によれば、端末では、証明書を発行するための紙などの印刷素材に付されたICチップや磁気カード（磁気部分）などの記録媒体に記憶されている識別情報を読み取り、証明書管理サーバで記録媒体が正当であるか否かを確認し、正当な記録媒体であれば、端末で紙などの印刷素材に証明書の内容を印刷して証明書を発行する。

【0012】また、請求項5では、印刷素材に付した記録媒体の識別情報を読み取る端末と前記記録媒体を管理する証明書管理サーバとがネットワークを介して接続し、前記証明書管理サーバは、前記記録媒体の識別情報

を前記端末から受信する識別情報受信手段と、前記識別情報を管理する識別情報データベースと、前記識別情報を前記識別情報データベースより検索して、正当であるか否かの真偽を判断する真偽判定手段と、真偽を判定し真の場合には前記端末で証明書を発行する真偽情報を前記端末に送信する真偽送信手段とを備える。

【0013】上記構成によれば、証明書管理サーバでは、受信した識別情報をもとに識別情報データベースで検索して、紙などの印刷素材に付された記録媒体が正当であるか否かを確認し、正当な記録媒体であれば、端末で印刷素材に証明書の内容を印刷するように端末に真偽情報を送信する。

【0014】また、請求項6では、記録媒体の識別情報を読み取る端末と前記記録媒体を管理する証明書管理サーバとがネットワークを介して接続し、前記端末は、前記記録媒体の識別情報を読み取る識別情報読み取り手段と、前記識別情報を前記証明書管理サーバに送信する識別情報送信手段とを備え、前記証明書管理サーバは、前記識別情報を管理する識別情報データベースと、前記識別情報より前記記録媒体が正当であるか否かを表す真偽情報を前記端末に送信する真偽送信手段とを備え、前記端末は、前記真偽情報が真の場合には、前記記録媒体に証明書の内容を記録して証明書を発行する証明書発行手段を備える。

【0015】上記構成によれば、ICカードや磁気カードなどの記録媒体に証明書を発行する端末と記録媒体を管理する証明書管理サーバがネットワークを介して接続され、端末で証明書を発行するために記録媒体に記憶された識別情報を読み取り、識別情報を証明書管理サーバに送信して、証明書管理サーバで記録媒体が正当であるか否かを確認し、正当な記録媒体であれば、端末でICカードや磁気カードなどの記録媒体に証明書の内容を記録して証明書を発行する。

【0016】また、請求項7では、請求項6記載の証明書発行システムにおいて、前記記録媒体は、識別情報を記憶したICカードであることを特徴とする。

【0017】上記構成では、ICカードを証明書として発行可能である。

【0018】また、請求項8では、記録媒体の識別情報を読み取る端末と前記記録媒体を管理する証明書管理サーバとがネットワークを介して接続し、前記端末は、前記記録媒体の識別情報を読み取る識別情報読み取り手段と、前記識別情報を前記証明書管理サーバに送信する識別情報送信手段と、前記記録媒体が正当であるか否かを表す真偽情報を前記証明書管理サーバから受信する真偽受信手段と、前記真偽情報が真の場合には、前記記録媒体が正当であると判断して前記記録媒体に証明書の内容を記録して証明書を発行する証明書発行手段とを備える。

【0019】上記構成では、端末では、ICチップや磁

気カード（磁気部分）などの記録媒体に記憶されている識別情報を読み取り、証明書管理サーバで記録媒体が正当であるか否かを確認し、正当な記録媒体であれば、端末で記録媒体に証明書の内容を記録して証明書を発行する。

【0020】また、請求項9では、記録媒体の識別情報を読み取る端末と前記記録媒体を管理する証明書管理サーバとがネットワークを介して接続し、前記証明書管理サーバは、前記記録媒体の識別情報を前記端末から受信する識別情報受信手段と、前記識別情報を管理する識別情報データベースと、前記識別情報を前記識別情報データベースより検索して、正当であるか否かの真偽を判断する真偽判定手段と、真偽を判定し真の場合には前記端末で証明書を発行する真偽情報を前記端末に送信する真偽送信手段とを備える。

【0021】上記構成では、証明書管理サーバでは、受信した識別情報をもとに識別情報データベースで検索して、ICチップや磁気カード（磁気部分）などの記録媒体が正当であるか否かを確認し、正当な記録媒体であれば、端末で印刷素材に証明書の内容を記録するように端末に真偽情報を送信する。

【0022】また、請求項10では、印刷素材に付された記録媒体の識別情報を読み取る識別情報読み取り手段と、識別情報を格納する識別情報データベースを備え、前記識別情報が正当であるか否かを前記識別情報データベースで検索して真偽を判断する真偽判断手段と、前記真偽情報が真の場合には、印刷素材に証明書の内容を印刷して証明書を発行する証明書発行手段を備える。

【0023】上記構成では、紙などの印刷素材に付されているICチップや磁気カード（磁気部分）などの記録媒体の識別情報を読み取り、識別情報を基に印刷素材が正当であるか否かを確認し、正当な記録媒体であれば、印刷素材に証明書の内容を印刷して証明書を発行する。

【0024】また、請求項11では、記録媒体の識別情報を読み取る識別情報読み取り手段と、識別情報を格納する識別情報データベースを備え、前記識別情報が正当であるか否かを前記識別情報データベースで検索して真偽を判断する真偽判断手段と、前記真偽情報が真の場合には、記録媒体に証明書の内容を記録して証明書を発行する証明書発行手段を備える。

【0025】上記構成では、ICチップや磁気カード（磁気部分）などの記録媒体の識別情報を読み取り、識別情報を基に印刷素材が正当であるか否かを確認し、正当な記録媒体であれば、記録媒体に証明書の内容を記憶して証明書を発行する。

【0026】

【発明の実施の形態】以下、本発明にかかる実施の形態を、図を用いて説明する。図1は、本発明の証明書発行システム1の構成を表す図である。証明書発行システム1は、予め用意された記録媒体31を付した印刷材料3

に証明書を印刷して発行する端末2と、記録媒体を管理する証明書管理サーバ4とネットワーク5から構成される。記録媒体31には識別情報が記憶され、証明書管理サーバ4には、識別情報を管理する識別情報データベース41を備える。以下本実施形態では、端末2は、コンビニエンスストアなどの店舗や代理店などに置かれ、自賠責保険などの保険証書類を発行する例を用いて説明する。また、記録媒体31を付した印刷素材3は保険会社などの証明書の発行を行う機関から、コンビニエンスストアなどの店舗や代理店に配布されるものである。

【0027】記録媒体31を付した印刷素材3とは、一例として、図2に示すように、紙に代表される印刷素材3にICチップや磁気カード（磁気部分）やバーコードやホログラムのような記録媒体31が付されている。つまり、ICチップなどの半導体が埋め込まれた紙、磁気カード（磁気部分）が付けられた紙、バーコードやホログラムなどが印刷された紙などである。ここで、ICチップとはCPU、メモリなどで構成されておりコンピュータ機能を持っている。また、ICチップにはアンテナを備え、非接触で入出力を行うことが可能なものや、ICチップに端子を備え、接触して入出力を行うものもある。

【0028】識別情報は、証明書を発行する保険会社などの機関で一意に割り振られるもので、ランダムに割り振った番号や暗号化したデータなどである。また、識別情報は、ICチップ（接触型、非接触型を含む）などの半導体や磁気カードなどの磁気部分に記憶される。或いは、バーコードやホログラムなどに情報として含まれるものである。また、ICチップなどの半導体には、書換不可能に記憶されることが望ましい。

【0029】端末2は、一例として、図3に示すように、コンビニエンスストアなどの店舗のレジ内7におかれ、パーソナルコンピュータなどの計算機203に、プリンターなどの印刷装置200に識別情報読み取り部204を備えたものを接続し、計算機203の通信機能を利用して証明書管理サーバ4と送受信するように構成する。また、印刷装置200は、図4に示すように、印刷部201と、識別情報読み取り部204と、計算機203と接続される通信部202と、を備えたものである。

【0030】識別情報読み取り部204は、各種の記録媒体3から記憶されている識別情報を読み取る装置で、ICカード読み取り装置（ICチップからの読み取りを含む）、磁気データ読み取り装置、ホログラム読み取り装置、バーコード読み取り装置などである。

【0031】また、記録媒体31に証明書の内容を追記する場合には、印刷装置200にICカード書き込み装置（ICチップへの書き込みを含む）や磁気カード書き込み装置を備えた構成としても良い。

【0032】また、端末2は、図5に示すように、コン

ビエンスストアなどの店舗のレジ内7にプリンターなどの印刷装置200をおき、通信部202に証明書管理サーバ4と送受信する機能を持たせるように構成しても良い。

【0033】或いは、コンビニエンスストアなどの店舗におかれる多機能情報端末で、発行するようにしても良い。

【0034】証明書管理サーバ4は、CPUなどの中央演算処理装置とRAMやROMなどのメモリと通信部などを備える計算機である。さらに、証明書管理サーバ4には、記録媒体31の識別情報32を管理する識別情報データベース41を備えている。通信部はネットワーク5と送受信を行う機能を備える。

【0035】また、端末2と証明書管理サーバ4とを接続するネットワーク5は、専用回線によって構成されるもの、ISDNなどの公衆回線によって構成されるもの、あるいは無線通信によって構成されるものなどの様々な回線形態を適用することが可能である。さらに、インターネットを利用して構成されるようにしてもよいが、情報管理の信頼性の観点から、セキュリティの確保されているネットワークであることが好ましい。

【0036】次に、証明書発行システム1の機能について図6に示すブロック図を用いて説明する。端末2は、識別情報読み取り部204でICチップなど記録媒体31に記憶されている識別情報32を読み取る識別情報読み取り手段26と、識別情報32を証明書管理サーバ4に送信する識別情報送信部27と、識別情報32が正当なものか否かを表す真偽情報33を証明書管理サーバ4から受信する真偽受信手段28と、印刷装置200を使って証明書を発行する証明書発行手段29とを備える。

【0037】証明書管理サーバ4は、配布された記録媒体3の識別情報32を管理する識別情報データベース41と、識別情報32を端末2から受信する識別情報受信手段42と、識別情報32が識別情報データベース41に該当するものがあるかを検索し真偽の判定をする真偽判定手段43と、真偽を表す真偽情報を端末2に送信する真偽送信手段44とを備える。また、真偽判定手段43では、識別情報が暗号化されている場合には解読処理を行うように構成しても良い。

【0038】次に、証明書発行システム1の動作について図7に示すフローチャートに基づき説明する。ここでは、ICチップ（記録媒体31）が埋め込まれた紙（印刷材料）3を使って保険会社が自賠責保険などの証明書を発行する場合を例に説明する。端末2は、コンビニエンスストアの店舗のレジ内7におかれ、パーソナルコンピュータなどの計算機203からプリンターなどの印刷装置200を利用して発行するものを例に説明する。さらに、ここでは、記録媒体31を非接触のICチップを用いたものとし、識別情報読み取り部204はICカード読み取り装置である。

【0039】まず、コンビニエンスストアなどの店舗には、ICチップ31が埋め込まれた紙3が保険会社から配布される。保険会社では事前に、識別情報32をICチップ31に記憶する。店舗のレジ内に置かれた印刷装置200にはICチップ31が埋め込まれた紙3がセットされる。

【0040】顧客から、自賠責保険の申込が行われ、申込が完了し保険金の収納（カードを利用する場合は、引き落としの確認）が確認されると、計算機203から証明書の発行の指示を印刷装置200に送る。印刷装置200は、証明書発行の指示を受け取ると、ICチップ31が埋め込まれた紙3が供給され、識別情報読み取り手段26で、ICカード読み取り装置（識別情報読み取り部）204から識別情報32の読み取る命令がICチップ31に発信される。ICチップ31からは識別情報32を発信し、ICカード読み取り装置204で受信する（S100）。識別情報送信手段27で、受信した識別情報32は通信部23から証明書管理サーバ4へ送信する（S101）。

【0041】証明書管理サーバ4では、識別情報受信手段42で識別情報32を受信し（S200）、真偽判定手段43では、識別情報32を識別情報データベースより検索し（S201）、正当な識別情報32かを判断する。識別情報32が暗号化されている場合には、解読して識別情報データベース41より検索し（S201）、正当な識別情報32かを判断する。識別情報32が正当であれば（S202）、真偽情報33を真とし（S203）、正当でなければ（S204）真偽情報33を偽とする（S205）。さらに、真偽送信手段44では、真偽情報33を端末2に送信する。

【0042】端末2では、真偽受信手段28で真偽情報33を通信部23で受信し（S102）、真偽情報33が真の場合は（S103）、証明書発行手段29でICチップが埋め込まれた紙3に証明書の内容をプリンター200で印刷して証明書を発行する（S104）。真偽情報33が偽の場合は（S103）、エラーを表示する（S106）。

【0043】さらに、証明書の印刷が終了すると証明書を発行したことを証明書管理サーバ4へ送信する（S105）。証明書管理サーバ4では、発行済みを受信し（S206）、識別情報データベース41に格納されている該当の識別情報32を発行済みにする（S207）。

【0044】また、ICチップ31が埋め込まれた紙3に証明書を印刷する際に、ICカード書き込み装置を印刷装置に備え、ICチップ31に必要な情報を書き込むようにしても良い。

【0045】以上説明したように、識別情報32より保険会社から配布された紙に対してのみ自賠責保険などの証明書を印刷する事が可能である。

【0046】また、自賠責保険の支払いや廃車に伴う返換金の支払いの時などに、ICチップに記憶されている情報（識別情報と含む）を読み取り、正当な証明書であることを確認するようにすることも可能である。

【0047】また、非接触のICチップを用いて説明したが接触型のICチップを利用してもよく、その際、ICチップの読み取り書き込み装置はICチップを読み書きする位置を固定できるように構成する。或いは、磁気カードを利用する際にも、磁気カード読み取り書き込み装置は磁気カードを読み書きする位置を固定できるように構成する。

【0048】さらに、識別情報32をバーコードやホログラムで印刷してある紙などの印刷材料としてもよく、この場合には、識別情報読み取り装置204はバーコード読み取り装置やホログラム読み取り装置とする。

【0049】以上詳細に説明したように、第1の実施の形態では、紙などの印刷材料に付された識別情報を確認して、保険会社から配布された正当なものか判断して自賠責保険などの証明書を印刷することが可能である。

【0050】次に、第2の実施の形態では、証明書を記録媒体31で発行する場合について説明する。前述の実施の形態と同じものについては同一符号を付して詳細な説明を省略する。図8に、第2の実施の形態の証明書発行システム1の構成を表す。第2の実施の形態では、端末2はICチップを埋め込んだICカードなどの記録媒体31で証明書を発行する。

【0051】また、端末2は、一例として、図9に示すように、パーソナルコンピュータなどの計算機203に、ICカード読み取り／書き込み装置などの記録媒体読み取り／書き込み装置200'を接続し、計算機203の通信機能を利用して証明書管理サーバ4と送受信するように構成する。

【0052】第2の実施の形態では、証明書発行システム1の機能は、図10に示すブロック図を用いて説明する。端末2は、識別情報読み取り手段26では、ICカード読み取り／書き込み装置などの記録媒体読み取り／書き込み装置200'でICカードなど記録媒体31に記憶されている識別情報32を読み取り、証明書発行手段29では、ICカード読み取り／書き込み装置などの記録媒体読み取り／書き込み装置200'を使って証明書を発行する。

【0053】また、記録媒体31は、プラスチックカードに、このICチップを埋め込んだICカード、或いは、プラスチックカードに磁気テープを付した磁気カード、CD-ROMやCD-RWなどの光ディスク、MO、MDやFDなどの磁気媒体が挙げられる。この記録媒体31には、識別情報32が予め保険会社などの証明書を発行する機関で一意に割り当てられ、証明書の内容が記録媒体31に追記されて証明書として発行される。

【0054】以下、ICカード（記録媒体）31を証明

書として発行する場合を例に説明する。ICカード31は、図11に示すように、プラスチックカードにICモジュール311が埋め込まれている。ICモジュール311は、データの入出力を行う端子312が設けられたICチップ313から構成されている。ICカード読み取り装置では、この端子312に接触してからデータの入出力を行う。或いは、この端子312がアンテナとなり非接触でデータの入出力を行う。

【0055】証明書発行システム1の動作を図7のフローチャートに基づき前述の実施例と相違する動作についてのみ詳細に説明する。顧客から、自賠責保険の申込が行われ、申込が完了し保険金の収納(カードを利用する場合は、引き落としの確認)が確認されると、証明書の発行の指示をICカード読み取り/書き込み装置200'に送る。ICカード読み取り/書き込み装置200'は、証明書発行の指示を受け取ると、ICカードが供給され、識別情報読み取り手段26で、ICカード読み取り/書き込み装置200'では、予め記憶されている識別情報32をICカード31から読み取る(S100)。識別情報送信手段27で、読み取った識別情報32を通信部23から証明書管理サーバ4へ送信する(S101)。

【0056】管理サーバ4の動作は、前述の実施の形態のS200～S205で説明したものと同様であるので詳細な説明は省略する。

【0057】管理サーバ4から送信された識別情報32が正当であるか否かを表す真偽情報33を端末2では、真偽受信手段28で受信し(S102)、真偽情報33が真の場合は(S103)、証明書発行手段29でICカード読み取り/書き込み装置200'でICカード31に証明書の内容を追記してICカード31を証明書として発行する(S104)。真偽情報33が偽の場合は(S103)、エラーを表示する(S106)。

【0058】さらに、証明書の印刷が終了すると証明書を発行したことを証明書管理サーバ4へ送信する(S105)。証明書管理サーバ4では、発行済みを受信し(S206)、識別情報データベース41に格納されている該当の識別情報32を発行済みにする(S207)。

【0059】以上詳細に説明したように、第2の実施の形態では、ICカードなどの記憶媒体で証明書を発行することができる。

【0060】次に、第3の実施の形態では、識別情報を各端末(証明書発行装置)で識別情報を管理して証明書を発行する場合について説明する。証明書発行装置は、図3で説明したように、コンビニエンスストアなどの店舗のレジ内7におかれ、パーソナルコンピュータなどの計算機203にプリンターなどの印刷装置200を備えたもの、或いは、図5で説明したように、コンビニエンスストアなどの店舗のレジ内7におかれるプリンタ

ーなどの印刷装置200である。また、コンビニエンスストアなどの店舗におかれる多機能情報端末である。

【0061】保険会社は、店舗に置かれた証明書発行装置にはICチップ31が埋め込まれた紙3をセットする。セットした紙3に埋め込まれているICチップ31の識別情報32は、FD(フロッピー(登録商標)ディスク)やCD-ROMなどの可搬型媒体によって証明書発行装置備えるハードディスクなどの記憶装置に登録する。

【0062】証明書発行装置2'の機能を、図12のブロック図を用いて説明する。証明書発行装置2'は、識別情報読み取り部204でICチップなど記録媒体31に記憶されている識別情報32を読み取る識別情報読み取り手段26と識別情報32が正当なものの否かを確認する真偽確認手段28'と、証明書発行部25を使って証明書を発行する証明書発行手段29とFD(フロッピーディスク)やCD-ROMなどの可搬型媒体から識別情報32を登録する識別情報データベース41'を備える。

【0063】次に、証明書発行装置2'の動作についてコンビニエンスストアなどの店舗のレジ内7におかれ、パーソナルコンピュータなどの計算機203にプリンターなどの印刷装置200を備えたものの証明書発行装置2'として利用して発行する場合を例に、図13に示すフローチャートに基づき説明する。さらに、ここでは、非接触のICチップが埋め込まれた紙に証明書を発行する場合について説明する。

【0064】顧客から、自賠責保険の申込が行われ、申込が完了し保険金の収納(カードを利用する場合は、引き落としの確認)が確認されると、計算機203から証明書の発行の指示を印刷装置200に送る。印刷装置は、証明書発行の指示を受け取ると、ICチップが埋め込まれた紙3が供給され、識別情報読み取り手段26で、ICカード読み取り装置(識別情報読み取り部)204でICチップから識別情報32の読み取る命令が発信される。ICチップからは識別情報32を発信し、ICカード読み取り装置204で受信する(S300)。

【0065】真偽確認手段28'では、識別情報32が、正当な紙か否かを判断する。また、識別情報32が暗号化されている場合には、解読して正当な識別情報32かを判断する(S301)。真偽情報33が真の場合は(S302)、証明書発行手段29でICチップが埋め込まれた紙3に証明書の内容をプリンター200で印刷して証明書を発行する(S303)。真偽情報33が偽の場合は(S302)、エラーを表示する(S304)。

【0066】また、ICチップが埋め込まれた紙3に証明書を印刷する際、ICカード書き込み装置を印刷装置に備え、ICチップに必要な情報を書き込むようにしても良い。

【0067】また、ICチップを用いて説明したが磁気カード（磁気部分）を利用するようにしても良い。また磁気カードを利用する際には、識別情報読み取り部204は磁気カード読み取り書き込み装置で構成する。

【0068】さらに、識別情報32をバーコードやホログラムで印刷してある紙などの印刷材料としてもよく、この場合には、識別情報読み取り部204はバーコード読み取り装置やホログラム読み取り装置とする。

【0069】FD（フロッピーディスク）やCD-ROMなどの可搬型媒体から識別情報をデータベースに登録する例を説明したが、FD（フロッピーディスク）やCD-ROMなどの可搬型媒体を証明書発行装置に設置し、識別情報を直接読み取るようにしても良い。

【0070】以上説明したように、第3の実施の形態では、ネットワークに接続しない装置でも識別情報を登録することにより保険会社から配布された紙が正当なのか判断して自賠責保険などの証明書を印刷することが可能である。

【0071】また、第2の実施の形態で説明したように、証明書発行装置2'で証明書を記録媒体31で発行するようにしても良い。この場合、証明書発行手段29でICカード書き込み装置などの記録媒体書き込み装置でICカードなどの記録媒体31に証明書の内容を追記してICカードを証明書として発行することも可能である。

【0072】第4の実施の形態では、コンビニエンスストアなどの店舗におかれる多機能情報端末で証明書を発行する場合について説明する。前述の実施の形態と同じものについては同一符号を付して詳細な説明を省略する。構成は、第1の実施の形態で図1を用いて説明した構成と同様である。また、端末2は、図3に示す端末2に替えて、図14に示すように印刷素材3に付されたICチップなど記録媒体31に記憶されている識別情報32を読み取る識別情報読み取り部204と、証明書を印刷する印刷部201とを備えたコンビニエンスストアなどの店舗におかれる多機能情報端末2'である。多機能情報端末2'は、チケットを発行する機能など多種類の機能を備えたものである。

【0073】多機能情報端末2'の機能は前述の実施の形態の端末2と同様である。また、証明書発行システム1の動作も前述の実施の形態と同様であるので詳細な説明は省略する。

【0074】また、証明書をICカードなどの記録媒体31で発行するようにしても良い。

【0075】以上説明したように、コンビニエンスストアなどの店舗におかれる多機能情報端末で、保険会社から配布された紙が正当なのか判断して自賠責保険などの証明書を印刷することが可能である。

【0076】

【発明の効果】以上説明したように、本発明では、店舗

や代理店などで不正に証明書を発行することを防ぐことができ、不正な支払いを行わないですむ。

【0077】また、白紙で配布された紙などの記録媒体が使用されなかったときに回収する手間や、使用されなかった紙などの記録媒体を廃棄するなどの無駄が省かれる。

【0078】さらに、記録媒体に記憶されている情報を読み取り、記憶されている情報を保険会社などに接続して確認することのより、確実に発行された証明書であることが確認できる。

【0079】さらに、証明書の内容自体を記録媒体で発行することが出来る。

【図面の簡単な説明】

【図1】 証明書発行システムの構成を表す図である。

【図2】 印刷素材に記録媒体が付されている図である。

【図3】 計算機と証明書管理サーバがネットワークで接続された図である。

【図4】 印刷装置の仕組みを表す図である。

【図5】 印刷装置と証明書管理サーバがネットワークで接続された図である。

【図6】 証明書発行システムの機能を表すブロック図である。

【図7】 証明書発行システムの動作を表すフローチャートである。

【図8】 第2の実施の形態の証明書発行システムの構成を表す図である。

【図9】 計算機と証明書管理サーバがネットワークで接続された図である。

【図10】 第2の実施の形態の証明書発行システムの機能を表すブロック図である。

【図11】 ICカードの構成を表す図である。

【図12】 証明書発行装置の機能を表すブロック図である。

【図13】 証明書発行装置の動作を表すフローチャートである。

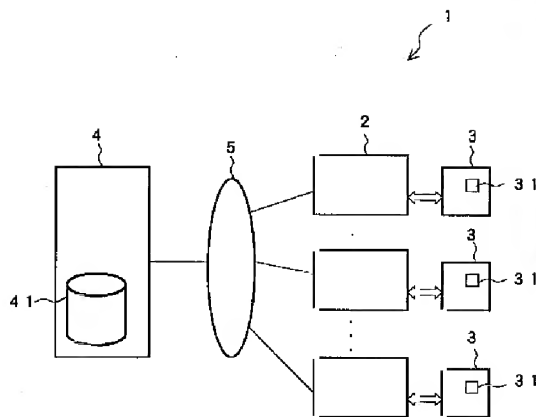
【図14】 多機能情報端末の仕組みを表す図である。

【符号の説明】

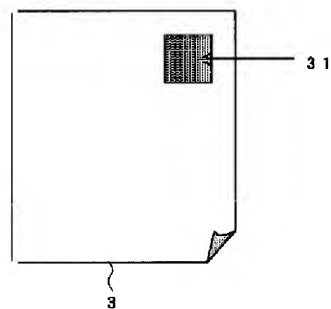
- 1 証明書発行システム
- 2 端末
- 2' 証明書発行装置
- 2'' 多機能情報端末
- 3 記録媒体
- 4 証明書管理サーバ
- 5 ネットワーク
- 7 店舗のレジ内
- 20 バスライン
- 21 中央演算処理装置（CPU）
- 22 メモリ
- 23 通信部

- | | |
|-------------------|----------------------|
| 26 識別情報読み取り手段 | 44 真偽送信手段 |
| 27 識別情報送信手段 | 200 印刷装置 |
| 28 真偽受信手段 | 200' 記録媒体読み取り／書き込み装置 |
| 28' 真偽確認手段 | 201 印刷部 |
| 29 証明書発行手段 | 202 通信部 |
| 31 記録媒体 | 203 計算機 |
| 32 識別情報 | 204 識別情報読み取り部 |
| 33 真偽情報 | 311 ICモジュール |
| 41、41' 識別情報データベース | 312 端子 |
| 42 識別情報受信手段 | 313 ICチップ |
| 43 真偽判定手段 | |

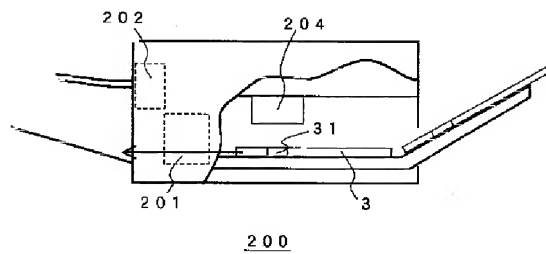
【図1】



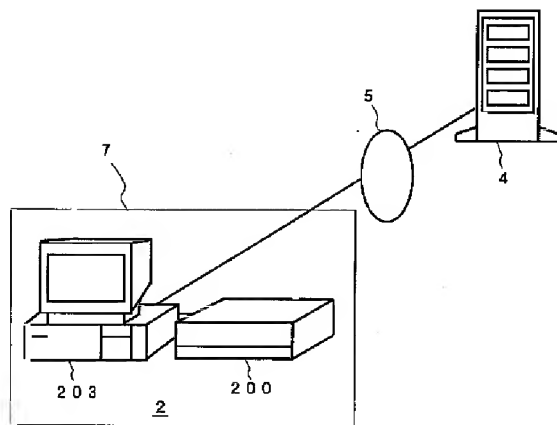
【図2】



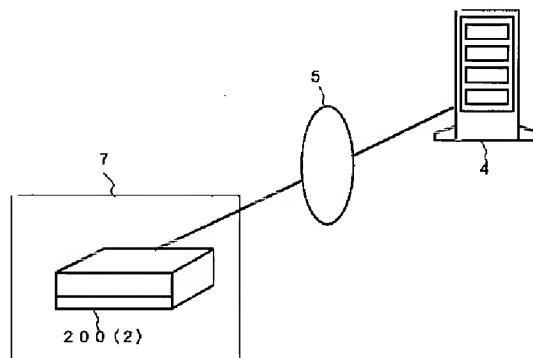
【図4】



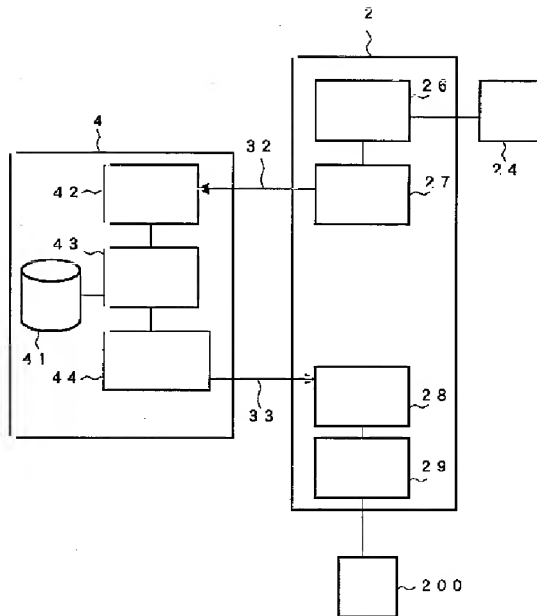
【図3】



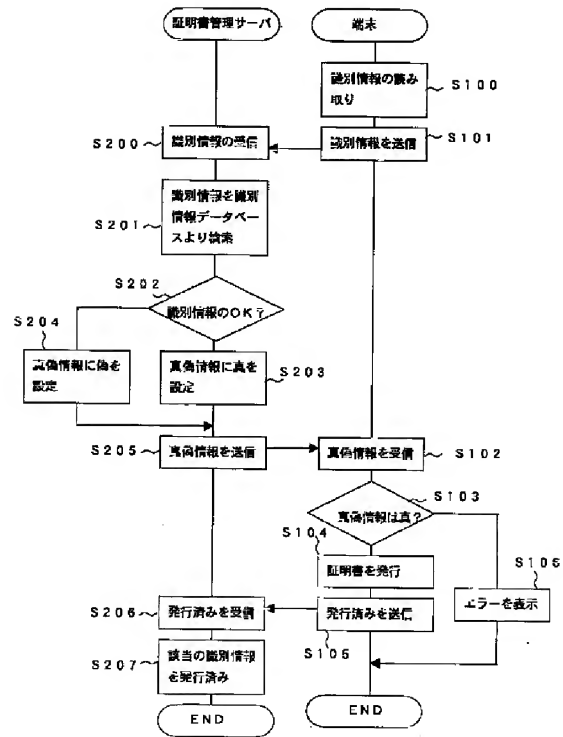
【図5】



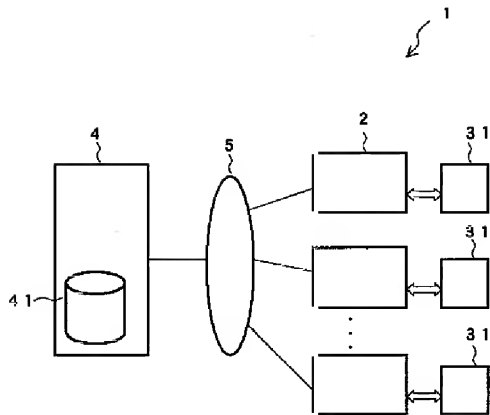
【図6】



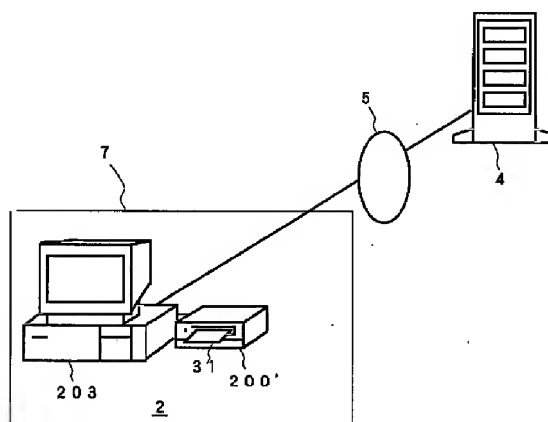
【図7】



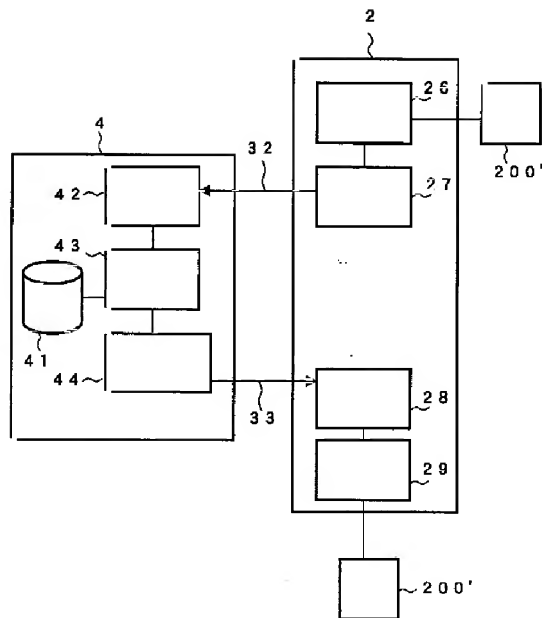
【図8】



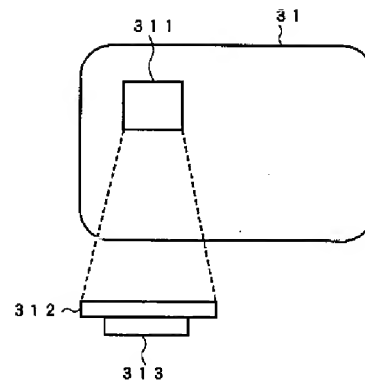
【図9】



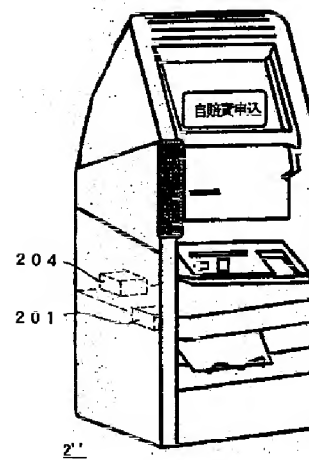
【図10】



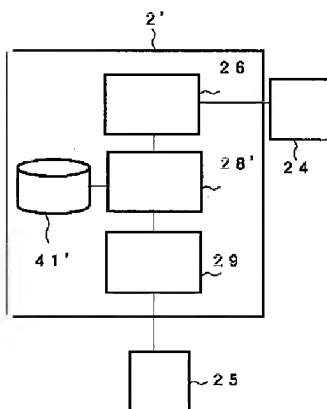
【図11】



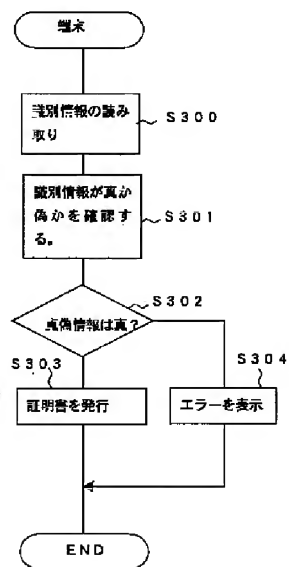
【図14】



【図12】



【図13】



【手続補正書】

【提出日】平成14年2月18日(2002.2.18)

【手続補正1】

【補正対象書類名】明細書

【補正対象項目名】全文

【補正方法】変更

【補正内容】

【書類名】明細書

【発明の名称】証明書発行システムおよび証明書発行装置

【特許請求の範囲】

【請求項1】 保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに保険会社の識別情報を記録したＩＣチップを付した保険会社専用の印刷素材を予めセットしておく端末と、前記印刷素材を管理する証明書管理サーバとをネットワークを介して接続し、前記端末は、前記識別情報を読み取る識別情報読み取り手段と、前記識別情報を前記証明書管理サーバに送信する識別情報送信手段とを備え、前記証明書管理サーバは、前記識別情報を管理する識別情報データベースと、前記識別情報より印刷素材が保険会社専用の印刷素材であるか否かを表す真偽情報を前記端末に送信する真偽送信手段とを備え、前記端末は、前記真偽情報が真の場合には、前記保険会社専用の印刷素材に保険会社の証明書の内容を印刷して保険会社の証明書を発行する証明書発行手段を備える証明書発行システム。

【請求項2】 請求項1記載の証明書発行システムにおいて、前記証明書発行手段で、前記ＩＣチップに保険会社の証明書の内容を記憶することを特徴とする証明書発行システム。

【請求項3】 保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに保険会社の識別情報を記録したＩＣチップを付した保険会社専用の印刷素材を予めセットしておく端末と、前記印刷素材を管理する証明書管理サーバとをネットワークを介して接続し、前記端末は、前記識別情報を読み取る識別情報読み取り手段と、前記識別情報を前記証明書管理サーバに送信する識別情報送信手段と、前記印刷素材が保険会社専用の印刷素材であるか否かを表す真偽情報を前記証明書管理サーバから受信する真偽受信手段と、前記真偽情報が真の場合には、前記識別情報が正当であると判断して保険会社専用の印刷素材に保険会社の証明書の内容を印刷して保険会社の証明書を発行する証明書発行手段とを備える証明書発行システム。

【請求項4】 保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに保険会社の識別情報を記録したＩＣチップを付した保険会社専用の印刷素材を予めセットしておく端末と、前記印刷素材を管理する証明書管理サーバとをネットワークを介して接続し、前記証明書管理サーバは、前記識別情報を前記端末から受信する識別情報受信手段と、前記識別情報を管理する識別情報データベースと、

前記識別情報を前記識別情報データベースで検索して、印刷素材が保険会社専用の印刷素材であるか否かの真偽を判断する真偽判定手段と、

真偽を判定し真の場合には前記端末で保険会社の証明書を前記保険会社専用の印刷素材に発行するために真偽情報を前記端末に送信する真偽送信手段とを備える証明書発行システム。

【請求項5】 保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに保険会社の識別情報を記録した保険会社専用のＩＣカードを予めセットしておく端末と、前記ＩＣカードを管理する証明書管理サーバとをネットワークを介して接続し、前記端末は、前記識別情報を読み取る識別情報読み取り手段と、前記識別情報を前記証明書管理サーバに送信する識別情報送信手段とを備え、前記証明書管理サーバは、前記識別情報を管理する識別情報データベースと、前記識別情報よりＩＣカードが保険会社専用のＩＣカードであるか否かを表す真偽情報を前記端末に送信する真偽送信手段とを備え、

前記端末は、前記真偽情報が真の場合には、前記保険会社専用のＩＣカードに保険会社の証明書の内容を記録して保険会社の証明書を発行する証明書発行手段を備える証明書発行システム。

【請求項6】 保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに保険会社の識別情報を記録した保険会社専用のＩＣカードを予めセットしておく端末と、前記ＩＣカードを管理する証明書管理サーバとをネットワークを介して接続し、前記端末は、前記識別情報を読み取る識別情報読み取り手段と、前記識別情報を前記証明書管理サーバに送信する識別情報送信手段と、前記ＩＣカードが保険会社のＩＣカードであるか否かを表す真偽情報を前記証明書管理サーバから受信する真偽受信手段と、

前記真偽情報が真の場合には、前記保険会社専用のＩＣカードに保険会社の証明書の内容を記録して保険会社の証明書を発行する証明書発行手段とを備える証明書発行システム。

【請求項7】 保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに保険会社の識別情報を記録した保険会社専用のＩＣカードを予めセットしておく端末と、前記ＩＣカードを管理する証明書管理サーバとをネットワークを介して接続し、前記証明書管理サーバは、前記識別情報を前記端末から受信する識別情報受信手段と、

前記識別情報を管理する識別情報データベースと、前記識別情報を前記識別情報データベースで検索して、ＩＣカードが保険会社専用のＩＣカードであるか否かの真偽を判断する真偽判定手段と、真偽を判定し真の場合には前記端末で前記保険会社専用のＩＣカードに保険会社の証明書を発行するための真偽情報を前記端末に送信する真偽送信手段とを備える証明書発行システム。

【請求項８】 保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに保険会社の識別情報を記録するＩＣチップを付した保険会社専用の印刷素材を予めセットし、前記識別情報を読み取る識別情報読み取り手段と、前記識別情報を格納する識別情報データベースと、前記識別情報が保険会社の識別情報であるか否かを前記識別情報データベースで検索して真偽を判断する真偽判断手段とを備え、前記真偽情報が真の場合には、前記保険会社専用の印刷素材に保険会社の証明書の内容を印刷して保険会社の証明書を発行する証明書発行手段を備える証明書発行装置。

【請求項９】 保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに保険会社の識別情報を記録する保険会社専用のＩＣカードを予めセットし、前記識別情報を読み取る識別情報読み取り手段と、前記識別情報を格納する識別情報データベースを備え、前記識別情報が正当であるか否かを前記識別情報データベースで検索して真偽を判断する真偽判断手段と、前記真偽情報が真の場合には、前記保険会社専用のＩＣカードに保険会社の証明書の内容を記録して保険会社の証明書を発行する証明書発行手段を備える証明書発行装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、証明書を発行するための証明書発行システム関する。

【０００２】

【従来の技術】従来は、自賠責保険などは、代理店で手書き、或いは、一部オフコンからドットプリンターで５枚綴りの帳票に印刷したものを証明書としていた。この証明書は、廃車などにともない不要になると解約することができ、解約に伴い返還金を受け取ることができる。

【０００３】

【発明が解決しようとする課題】そこで、代理店などでこの帳票を不正に使用して偽造し、この返還金を受け取ることが可能である。この偽造を防ぐために、常に、帳票の管理を行わなければ行けない。例えば、代理店に置く帳票の枚数を保険会社が管理し、数か月単位で回収して、その代理店から申し込まれた自賠責保険の件数と残っている帳票の数の合計が、始めに置いた帳票の枚数

と一致しなければならない。また、代理店で書き損じ（書損）の帳票も必ず取っておく必要があり大変煩わしかった。さらに、この回収と書損に伴い、現在保険会社から白紙で配布された帳票の内約３～４割が廃棄され無駄が多かった。

【０００４】

【課題を解決するための手段】前述の課題を解決するため、本発明に係る証明書発行システムの、請求項１では、保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに保険会社の識別情報を記録したＩＣチップを付した保険会社専用の印刷素材を予めセットしておく端末と、前記印刷素材を管理する証明書管理サーバとをネットワークを介して接続し、前記端末は、前記識別情報を読み取る識別情報読み取り手段と、前記識別情報を前記証明書管理サーバに送信する識別情報送信手段とを備え、前記証明書管理サーバは、前記識別情報を管理する識別情報データベースと、前記識別情報より印刷素材が保険会社専用の印刷素材であるか否かを表す真偽情報を前記端末に送信する真偽送信手段とを備え、前記端末は、前記真偽情報が真の場合には、前記保険会社専用の印刷素材に保険会社の証明書の内容を印刷して保険会社の証明書を発行する証明書発行手段を備える。

【０００５】上記構成によれば、ＩＣチップを付した紙など印刷可能な素材である印刷素材のＩＣチップに保険会社の識別情報を記録した保険会社専用の印刷素材を端末に予めセットし、この端末とＩＣチップに記録された識別情報を管理する証明書管理サーバがネットワークを介して接続し、端末で証明書を発行するためにＩＣチップに記憶された識別情報を読み取り、識別情報を証明書管理サーバに送信して、証明書管理サーバで印刷素材が保険会社専用のものであるか否かを確認し、保険会社専用の印刷素材であれば、端末で印刷素材に保険会社の証明書の内容を印刷して証明書を発行する。証明書とは、保険証書類である。

【０００６】また、請求項２では、請求項１記載の証明書発行システムにおいて、前記証明書発行手段で、前記ＩＣチップに保険会社の証明書の内容を記憶することを特徴とする。

【０００７】上記構成によれば、証明書を印刷するだけでなく必要に応じてＩＣチップに保険会社の証明書の内容を記録することが可能である。

【０００８】また、請求項３では、保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに保険会社の識別情報を記録したＩＣチップを付した保険会社専用の印刷素材を予めセットしておく端末と、前記印刷素材を管理する証明書管理サーバとをネットワークを介して接続し、前記端末は、前記識別情報を読み取る識別情報読み取り手段と、前記識別情報を前記証明書管理サーバに送信する識別情報送信手段と、前記印刷素

材が保険会社専用の印刷素材であるか否かを表す真偽情報を前記証明書管理サーバから受信する真偽受信手段と、前記真偽情報が真の場合には、前記識別情報が正当であると判断して保険会社専用の印刷素材に保険会社の証明書の内容を印刷して保険会社の証明書を発行する証明書発行手段とを備える。

【 〇 〇 〇 9 】 上記構成によれば、保険会社の証明書を発行するための紙などの印刷素材に付された I C チップには保険会社の識別情報が記憶されており、端末には、この保険会社専用の印刷素材が予めセットされ、端末にセットされた印刷素材の識別情報を読み取り、証明書管理サーバで識別情報から印刷素材が保険会社のものであるか否かを確認し、保険会社の識別情報であれば、端末で紙などの印刷素材に保険会社の証明書の内容を印刷して証明書を発行する。

【 〇 〇 1 〇 】 また、請求項 4 では、保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに、保険会社の識別情報を記録した I C チップを付した保険会社専用の印刷素材を予めセットしておく端末と、前記印刷素材を管理する証明書管理サーバとをネットワークを介して接続し、前記証明書管理サーバは、前記識別情報を前記端末から受信する識別情報受信手段と、前記識別情報を管理する識別情報データベースと、前記識別情報を前記識別情報データベースで検索して、印刷素材が保険会社専用の印刷素材であるか否かの真偽を判断する真偽判定手段と、真偽を判定し真の場合には前記端末で保険会社の証明書を前記保険会社専用の印刷素材に発行するために真偽情報を前記端末に送信する真偽送信手段とを備える。

【 〇 〇 1 1 】 上記構成によれば、証明書管理サーバでは、受信した識別情報をもとに識別情報データベースで検索して、紙などの印刷素材に付された I C チップの識別情報から印刷素材が保険会社専用のものであるか否かを確認し、保険会社の識別情報であれば、端末で印刷素材に保険会社の証明書の内容を印刷するように端末に真偽情報を送信する。

【 〇 〇 1 2 】 また、請求項 5 では、保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに、保険会社の識別情報を記録した保険会社専用の I C カードを予めセットしておく端末と、前記 I C カードを管理する証明書管理サーバとをネットワークを介して接続し、前記端末は、前記識別情報を読み取る識別情報読み取り手段と、前記識別情報を前記証明書管理サーバに送信する識別情報送信手段とを備え、前記証明書管理サーバは、前記識別情報を管理する識別情報データベースと、前記識別情報より I C カードが保険会社専用の I C カードであるか否かを表す真偽情報を前記端末に送信する真偽送信手段とを備え、前記端末は、前記真偽情報が真の場合には、前記保険会社専用の I C カードに保険会社の証明書の内容を記録して保険会社の証明書を発行す

る証明書発行手段を備える。

【 〇 〇 1 3 】 上記構成によれば、保険会社の識別情報を記録した保険会社専用の I C カードを予めセットした端末と I C カードを管理する証明書管理サーバがネットワークを介して接続され、端末で保険会社の証明書を発行するために I C カードに記憶された識別情報を読み取り、識別情報を証明書管理サーバに送信して、証明書管理サーバで I C カードが保険会社専用であるか否かを確認し、保険会社専用の I C カードであれば、端末で I C カードに保険会社の証明書の内容を記録して証明書を発行する。

【 〇 〇 1 4 】 また、請求項 6 では、保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに、保険会社の識別情報を記録した保険会社専用の I C カードを予めセットしておく端末と、前記 I C カードを管理する証明書管理サーバとをネットワークを介して接続し、前記端末は、前記識別情報を読み取る識別情報読み取り手段と、前記識別情報を前記証明書管理サーバに送信する識別情報送信手段と、前記 I C カードが保険会社の I C カードであるか否かを表す真偽情報を前記証明書管理サーバから受信する真偽受信手段と、前記真偽情報が真の場合には、前記保険会社専用の I C カードに保険会社の証明書の内容を記録して保険会社の証明書を発行する証明書発行手段とを備える。

【 〇 〇 1 5 】 上記構成では、端末には保険会社の識別情報を記録した保険会社専用の I C カードが予めセットされ、I C カードに記憶されている識別情報を読み取り、証明書管理サーバで I C カードが保険会社専用であるか否かを確認し、保険会社専用の I C カードであれば、端末で I C カードに保険会社の証明書の内容を記録して証明書を発行する。

【 〇 〇 1 6 】 また、請求項 7 では、保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに、保険会社の識別情報を記録した保険会社専用の I C カードを予めセットしておく端末と、前記 I C カードを管理する証明書管理サーバとをネットワークを介して接続し、前記証明書管理サーバは、前記識別情報を前記端末から受信する識別情報受信手段と、前記識別情報を管理する識別情報データベースと、前記識別情報を前記識別情報データベースで検索して、I C カードが保険会社専用の I C カードであるか否かの真偽を判断する真偽判定手段と、真偽を判定し真の場合には前記端末で前記保険会社専用の I C カードに保険会社の証明書を発行するための真偽情報を前記端末に送信する真偽送信手段とを備える。

【 〇 〇 1 7 】 上記構成では、証明書管理サーバでは、受信した識別情報をもとに識別情報データベースで検索して、I C カードが保険会社専用であるか否かを確認し、保険会社専用の I C カードであれば、端末で I C カードに保険会社の証明書の内容を記録するように端末に真偽

情報を送信する。

【0018】また、請求項8では、保険会社の代理店やコンビニエンスストアなどの店舗に置かれるとともに保険会社の識別情報を記録するICチップを付した保険会社専用の印刷素材を予めセットし、前記識別情報を読み取る識別情報読み取り手段と、前記識別情報を格納する識別情報データベースと、前記識別情報が保険会社の識別情報であるか否かを前記識別情報データベースで検索して真偽を判断する真偽判断手段とを備え、前記真偽情報が真の場合には、前記保険会社専用の印刷素材に保険会社の証明書の内容を印刷して保険会社の証明書を発行する証明書発行手段を備える。

【0019】上記構成では、紙などの印刷素材に付されているICチップには保険会社の識別情報が記憶され、この印刷素材を予めセットしておき、このICチップの識別情報を読み取り、識別情報を基に印刷素材が保険会社専用のものであるか否かを確認し、保険会社専用の印刷素材であれば、印刷素材に保険会社の証明書の内容を印刷して証明書を発行する。

【0020】また、請求項9では、保険会社の代理店やコンビニエンスストアなどの店舗に置かれ、保険会社の識別情報を記録する保険会社専用のICカードを予めセットし、前記識別情報を読み取る識別情報読み取り手段と、前記識別情報を格納する識別情報データベースを備え、前記識別情報が正当であるか否かを前記識別情報データベースで検索して真偽を判断する真偽判断手段と、前記真偽情報が真の場合には、前記保険会社専用のICカードに保険会社の証明書の内容を記録して保険会社の証明書を発行する証明書発行手段を備える。

【0021】上記構成では、保険会社の識別情報が記録された保険会社専用のICカードを予めセットし、ICカードの識別情報を読み取り、識別情報を基にICカードが保険会社専用であるか否かを確認し、保険会社専用のICカードであれば保険会社の証明書の内容を記憶して証明書を発行する。

【0022】

【発明の実施の形態】以下、本発明にかかる実施の形態を、図を用いて説明する。図1は、本発明の証明書発行システム1の構成を表す図である。証明書発行システム1は、予め用意された記録媒体31を付した印刷材料3に証明書を印刷して発行する端末2と、記録媒体を管理する証明書管理サーバ4とネットワーク5から構成される。記録媒体31には識別情報が記憶され、証明書管理サーバ4には、識別情報を管理する識別情報データベース41を備える。以下本実施形態では、端末2は、コンビニエンスストアなどの店舗や代理店などに置かれ、自賠責保険などの保険証書類を発行する例を用いて説明する。また、記録媒体31を付した印刷素材3は保険会社などの証明書の発行を行う機関から、コンビニエンスストアなどの店舗や代理店に配布されるものである。

【0023】記録媒体31を付した印刷素材3とは、一例として、図2に示すように、紙に代表される印刷素材3にICチップや磁気カード（磁気部分）やバーコードやホログラムのような記録媒体31が付されている。つまり、ICチップなどの半導体が埋め込まれた紙、磁気カード（磁気部分）が付けられた紙、バーコードやホログラムなどが印刷された紙などである。ここで、ICチップとはCPU、メモリなどで構成されておりコンピュータ機能を持っている。また、ICチップにはアンテナを備え、非接触で入出力を行うことが可能なものや、ICチップに端子を備え、接触して入出力を行うものもある。

【0024】識別情報は、証明書を発行する保険会社などの機関で一意に割り振られるもので、ランダムに割り振った番号や暗号化したデータなどである。また、識別情報は、ICチップ（接触型、非接触型を含む）などの半導体や磁気カードなどの磁気部分に記憶される。或いは、バーコードやホログラムなどに情報として含まれるものである。また、ICチップなどの半導体には、書換不可能に記憶されることが望ましい。

【0025】端末2は、一例として、図3に示すように、コンビニエンスストアなどの店舗のレジ内7におかれ、パーソナルコンピュータなどの計算機203に、プリンターなどの印刷装置200に識別情報読み取り部204を備えたものを接続し、計算機203の通信機能を利用して証明書管理サーバ4と送受信するように構成する。また、印刷装置200は、図4に示すように、印刷部201と、識別情報読み取り部204と、計算機203と接続される通信部202と、を備えたものである。

【0026】識別情報読み取り部204は、各種の記録媒体3から記憶されている識別情報を読み取る装置で、ICカード読み取り装置（ICチップからの読み取りを含む）、などである。

【0027】識別情報読み取り部204は、各種の記録媒体3から記憶されている識別情報を読み取る装置で、ICカード読み取り装置（ICチップからの読み取りを含む）、磁気データ読み取り装置、ホログラム読み取り装置、バーコード読み取り装置などである。

【0028】また、端末2は、図5に示すように、コンビニエンスストアなどの店舗のレジ内7にプリンターなどの印刷装置200をおき、通信部202に証明書管理サーバ4と送受信する機能を持たせるように構成しても良い。

【0029】或いは、コンビニエンスストアなどの店舗におかれる多機能情報端末で、発行するようにしても良い。

【0030】証明書管理サーバ4は、CPUなどの中央演算処理装置とRAMやROMなどのメモリと通信部などを備える計算機である。さらに、証明書管理サーバ4

には、記録媒体31の識別情報32を管理する識別情報データベース41を備えている。通信部はネットワーク5と送受信を行う機能を備える。

【0031】また、端末2と証明書管理サーバ4とを接続するネットワーク5は、専用回線によって構成されるもの、ISDNなどの公衆回線によって構成されるもの、あるいは無線通信によって構成されるものなどの様々な回線形態を適用することが可能である。さらに、インターネットを利用して構成されるようにしてもよいが、情報管理の信頼性の観点から、セキュリティの確保されているネットワークであることが好ましい。

【0032】次に、証明書発行システム1の機能について図6に示すブロック図を用いて説明する。端末2は、識別情報読み取り部204でICチップなど記録媒体31に記憶されている識別情報32を読み取る識別情報読み取り手段26と、識別情報32を証明書管理サーバ4に送信する識別情報送信部27と、識別情報32が正当なものか否かを表す真偽情報33を証明書管理サーバ4から受信する真偽受信手段28と、印刷装置200を使って証明書を発行する証明書発行手段29とを備える。

【0033】証明書管理サーバ4は、配布された記録媒体3の識別情報32を管理する識別情報データベース41と、識別情報32を端末2から受信する識別情報受信手段42と、識別情報32が識別情報データベース41に該当するものがあるかを検索し真偽の判定をする真偽判定手段43と、真偽を表す真偽情報を端末2に送信する真偽送信手段44とを備える。また、真偽判定手段43では、識別情報が暗号化されている場合には解読処理を行うように構成しても良い。

【0034】次に、証明書発行システム1の動作について図7に示すフローチャートに基づき説明する。ここでは、ICチップ（記録媒体31）が埋め込まれた紙（印刷材料）3を使って保険会社が自賠責保険などの証明書を発行する場合を例に説明する。端末2は、コンビニエンスストアの店舗のレジ内7におかれ、パーソナルコンピュータなどの計算機203からプリンターなどの印刷装置200を利用して発行するものを例に説明する。さらに、ここでは、記録媒体31を非接触のICチップを用いたものとし、識別情報読み取り部204はICカード読み取り装置である。

【0035】まず、コンビニエンスストアなどの店舗には、ICチップ31が埋め込まれた紙3が保険会社から配布される。保険会社では事前に、識別情報32をICチップ31に記憶する。店舗のレジ内に置かれた印刷装置200にはICチップ31が埋め込まれた紙3がセットされる。

【0036】顧客から、自賠責保険の申込が行われ、申込が完了し保険金の収納（カードを利用する場合は、引き落としの確認）が確認されると、計算機203から証明書の発行の指示を印刷装置200に送る。印刷装置2

00は、証明書発行の指示を受け取ると、ICチップ31が埋め込まれた紙3が供給され、識別情報読み取り手段26で、ICカード読み取り装置（識別情報読み取り部）204から識別情報32の読み取る命令がICチップ31に発信される。ICチップ31からは識別情報32を発信し、ICカード読み取り装置204で受信する（S100）。識別情報送信手段27で、受信した識別情報32は通信部23から証明書管理サーバ4へ送信する（S101）。

【0037】証明書管理サーバ4では、識別情報受信手段42で識別情報32を受信し（S200）、真偽判定手段43では、識別情報32を識別情報データベースより検索し（S201）、正当な識別情報32かを判断する。識別情報32が暗号化されている場合には、解読して識別情報データベース41より検索し（S201）、正当な識別情報32かを判断する。識別情報32が正当であれば（S202）、真偽情報33を真とし（S203）、正当でなければ（S204）真偽情報33を偽とする（S205）。さらに、真偽送信手段44では、真偽情報33を端末2に送信する。

【0038】端末2では、真偽受信手段28で真偽情報33を通信部23で受信し（S102）、真偽情報33が真の場合は（S103）、証明書発行手段29でICチップが埋め込まれた紙3に証明書の内容をプリンター200で印刷して証明書を発行する（S104）。真偽情報33が偽の場合は（S103）、エラーを表示する（S106）。

【0039】さらに、証明書の印刷が終了すると証明書を発行したことを証明書管理サーバ4へ送信する（S105）。証明書管理サーバ4では、発行済みを受信し（S206）、識別情報データベース41に格納されている該当の識別情報32を発行済みにする（S207）。

【0040】また、ICチップ31が埋め込まれた紙3に証明書を印刷する際に、ICカード書き込み装置を印刷装置に備え、ICチップ31に必要な情報を書き込むようにしても良い。

【0041】以上説明したように、識別情報32より保険会社から配布された紙対してのみ自賠責保険などの証明書を印刷する事が可能である。

【0042】また、自賠責保険の支払いや廃車に伴う返換金の支払いの時などに、ICチップに記憶されている情報（識別情報と含む）を読み取り、正当な証明書であることを確認するようにすることも可能である。

【0043】また、非接触のICチップを用いて説明したが接触型のICチップを利用してもよく、その際、ICチップの読み取り書き込み装置はICチップを読み書きする位置を固定できるように構成する。或いは、磁気カードを利用する際にも、磁気カード読み取り書き込み装置は磁気カードを読み書きする位置を固定できるよう

に構成する。

【0044】さらに、識別情報32をバーコードやホログラムで印刷してある紙などの印刷材料としてもよく、この場合には、識別情報読み取り装置204はバーコード読み取り装置やホログラム読み取り装置とする。

【0045】以上詳細に説明したように、第1の実施の形態では、紙などの印刷材料に付された識別情報を確認して、保険会社から配布された正当なものか判断して自賠責保険などの証明書を印刷することが可能である。

【0046】次に、第2の実施の形態では、証明書を記録媒体31で発行する場合について説明する。前述の実施の形態と同じものについては同一符号を付して詳細な説明を省略する。図8に、第2の実施の形態の証明書発行システム1の構成を表す。第2の実施の形態では、端末2はICチップを埋め込んだICカードなどの記録媒体31で証明書を発行する。

【0047】また、端末2は、一例として、図9に示すように、パーソナルコンピュータなどの計算機203に、ICカード読み取り／書き込み装置などの記録媒体読み取り／書き込み装置200'を接続し、計算機203の通信機能を利用して証明書管理サーバ4と送受信するように構成する。

【0048】第2の実施の形態では、証明書発行システム1の機能は、図10に示すブロック図を用いて説明する。端末2は、識別情報読み取り手段26では、ICカード読み取り／書き込み装置などの記録媒体読み取り／書き込み装置200'でICカードなど記録媒体31に記憶されている識別情報32を読み取り、証明書発行手段29では、ICカード読み取り／書き込み装置などの記録媒体読み取り／書き込み装置200'を使って証明書を発行する。

【0049】また、記録媒体31は、プラスチックカードに、このICチップを埋め込んだICカード、或いは、プラスチックカードに磁気テープを付した磁気カード、CD-ROMやCD-RWなどの光ディスク、MO、MDやFDなどの磁気媒体が挙げられる。この記録媒体31には、識別情報32が予め保険会社などの証明書を発行する機関で一意に割り当てられ、証明書の内容が記録媒体31に追記されて証明書として発行される。

【0050】以下、ICカード（記録媒体）31を証明書として発行する場合を例に説明する。ICカード31は、図11に示すように、プラスチックカードにICモジュール311が埋め込まれている。ICモジュール311は、データの入出力を行う端子312が設けられたICチップ313から構成されている。ICカード読み取り装置では、この端子312に接触してからデータの入出力を行う。或いは、この端子312がアンテナとなり非接触でデータの入出力を行う。

【0051】証明書発行システム1の動作を図7のフローチャートに基づき前述の実施例と相違する動作につい

てのみ詳細に説明する。顧客から、自賠責保険の申込が行われ、申込が完了し保険金の収納（カードを利用する場合は、引き落としの確認）が確認されると、証明書の発行の指示をICカード読み取り／書き込み装置200'に送る。ICカード読み取り／書き込み装置200'は、証明書発行の指示を受け取ると、ICカードが供給され、識別情報読み取り手段26で、ICカード読み取り／書き込み装置200'では、予め記憶されている識別情報32をICカード31から読み取る（S100）。識別情報送信手段27で、読み取った識別情報32を通信部23から証明書管理サーバ4へ送信する（S101）。

【0052】管理サーバ4の動作は、前述の実施の形態のS200～S205で説明したものと同様であるので詳細な説明は省略する。

【0053】管理サーバ4から送信された識別情報32が正当であるか否かを表す真偽情報33を端末2では、真偽受信手段28で受信し（S102）、真偽情報33が真の場合は（S103）、証明書発行手段29でICカード読み取り／書き込み装置200'でICカード31に証明書の内容を追記してICカード31を証明書として発行する（S104）。真偽情報33が偽の場合は（S103）、エラーを表示する（S106）。

【0054】さらに、証明書の印刷が終了すると証明書を発行したことを証明書管理サーバ4へ送信する（S105）。証明書管理サーバ4では、発行済みを受信し（S206）、識別情報データベース41に格納されている該当の識別情報32を発行済みにする（S207）。

【0055】以上詳細に説明したように、第2の実施の形態では、ICカードなどの記憶媒体で証明書を発行することができる。

【0056】次に、第3の実施の形態では、識別情報を各端末（証明書発行装置）で識別情報を管理して証明書を発行する場合について説明する。証明書発行装置は、図3で説明したように、コンビニエンスストアなどの店舗のレジ内7におかれ、パーソナルコンピュータなどの計算機203にプリンターなどの印刷装置200を備えたもの、或いは、図5で説明したように、コンビニエンスストアなどの店舗のレジ内7におかれるプリンターなどの印刷装置200である。また、コンビニエンスストアなどの店舗におかれる多機能情報端末である。

【0057】保険会社は、店舗に置かれた証明書発行装置にはICチップ31が埋め込まれた紙3をセットする。セットした紙3に埋め込まれているICチップ31の識別情報32は、FD（フロッピーディスク）やCD-ROMなどの可搬型媒体によって証明書発行装置備えるハードディスクなどの記憶装置に登録する。

【0058】証明書発行装置2'の機能を、図12のブロック図を用いて説明する。証明書発行装置2'は、識

別情報読み取り部204でICチップなど記録媒体31に記憶されている識別情報32を読み取る識別情報読み取り手段26と識別情報32が正当なものか否かを確認する真偽確認手段28'と、証明書発行部25を使って証明書を発行する証明書発行手段29とFD（フロッピーディスク）やCD-ROMなどの可搬型媒体から識別情報32を登録する識別情報データベース41'を備える。

【0059】次に、証明書発行装置2'の動作についてコンビニエンスストアなどの店舗のレジ内7におかれ、パーソナルコンピュータなどの計算機203にプリンターなどの印刷装置200を備えたもの証明書発行装置2'として利用して発行する場合を例に、図13に示すフローチャートに基づき説明する。さらに、ここでは、非接触のICチップが埋め込まれた紙に証明書を発行する場合について説明する。

【0060】顧客から、自賠責保険の申込が行われ、申込が完了し保険金の収納（カードを利用する場合は、引き落としの確認）が確認されると、計算機203から証明書の発行の指示を印刷装置200に送る。印刷装置は、証明書発行の指示を受け取ると、ICチップが埋め込まれた紙3が供給され、識別情報読み取り手段26で、ICカード読み取り装置（識別情報読み取り部）204でICチップから識別情報32の読み取る命令が発信される。ICチップからは識別情報32を発信し、ICカード読み取り装置204で受信する（S300）。

【0061】真偽確認手段28'では、識別情報32が、正当な紙か否かを判断する。また、識別情報32が暗号化されている場合には、解読して正当な識別情報32かを判断する（S301）。真偽情報33が真の場合は（S302）、証明書発行手段29でICチップが埋め込まれた紙3に証明書の内容をプリンター200で印刷して証明書を発行する（S303）。真偽情報33が偽の場合は（S302）、エラーを表示する（S304）。

【0062】また、ICチップが埋め込まれた紙3に証明書を印刷する際、ICカード書き込み装置を印刷装置に備え、ICチップに必要な情報を書き込むようにしても良い。

【0063】また、ICチップを用いて説明したが磁気カード（磁気部分）を利用するようにしても良い。また磁気カードを利用する際には、識別情報読み取り部204は磁気カード読み取り書き込み装置で構成する。

【0064】さらに、識別情報32をバーコードやホログラムで印刷してある紙などの印刷材料としてもよく、この場合には、識別情報読み取り部204はバーコード読み取り装置やホログラム読み取り装置とする。

【0065】FD（フロッピーディスク）やCD-ROMなどの可搬型媒体から識別情報をデータベースに登録する例を説明したが、FD（フロッピーディスク）やC

D-ROMなどの可搬型媒体を証明書発行装置に設置し、識別情報を直接読み取るようにしても良い。

【0066】以上説明したように、第3の実施の形態では、ネットワークに接続しない装置でも識別情報を登録することにより保険会社から配布された紙が正当なものか判断して自賠責保険などの証明書を印刷することが可能である。

【0067】また、第2の実施の形態で説明したように、証明書発行装置2'で証明書を記録媒体31で発行するようにしても良い。この場合、証明書発行手段29でICカード書き込み装置などの記録媒体書き込み装置でICカードなどの記録媒体31に証明書の内容を追記してICカードを証明書として発行することも可能である。

【0068】第4の実施の形態では、コンビニエンスストアなどの店舗におかれる多機能情報端末で証明書を発行する場合について説明する。前述の実施の形態と同じものについては同一符号を付して詳細な説明を省略する。構成は、第1の実施の形態で図1を用いて説明した構成と同様である。また、端末2は、図3に示す端末2に替えて、図14に示すように印刷素材3に付されたICチップなど記録媒体31に記憶されている識別情報32を読み取る識別情報読み取り部204と、証明書を印刷する印刷部201とを備えたコンビニエンスストアなどの店舗におかれる多機能情報端末2'である。多機能情報端末2'は、チケットを発行する機能など多種類の機能を備えたものである。

【0069】多機能情報端末2'の機能は前述の実施の形態の端末2と同様である。また、証明書発行システム1の動作も前述の実施の形態と同様であるので詳細な説明は省略する。

【0070】また、証明書をICカードなどの記録媒体31で発行するようにしても良い。

【0071】以上説明したように、コンビニエンスストアなどの店舗におかれる多機能情報端末で、保険会社から配布された紙が正当なものか判断して自賠責保険などの証明書を印刷することが可能である。

【0072】

【発明の効果】以上説明したように、本発明では、コンビニエンスストアなどの店舗や保険会社の代理店に置かれる端末に、保険会社専用の印刷素材やICカードを予めセットすることで不正に証明書を発行することを防ぐことができ、不正な支払いを行わないですむ。

【0073】また、白紙で配布された紙などの印刷素材やICカードが使用されなかったときに回収する手間や、使用されなかった紙などの印刷素材やICカードを廃棄するなどの無駄が省かれる。

【0074】さらに、記録媒体に記憶されている識別情報を読み取り、記憶されている情報を保険会社などに接続して確認することにより、確実に発行された証明書で

あることが確認できる。

【0075】さらに、証明書の内容自体を記録媒体で発行することが出来る。

【図面の簡単な説明】

【図1】 証明書発行システムの構成を表す図である。

【図2】 印刷素材に記録媒体が付されている図である。

【図3】 計算機と証明書管理サーバがネットワークで接続された図である。

【図4】 印刷装置の仕組みを表す図である。

【図5】 印刷装置と証明書管理サーバがネットワークで接続された図である。

【図6】 証明書発行システムの機能を表すブロック図である。

【図7】 証明書発行システムの動作を表すフローチャートである。

【図8】 第2の実施の形態の証明書発行システムの構成を表す図である。

【図9】 計算機と証明書管理サーバがネットワークで接続された図である。

【図10】 第2の実施の形態の証明書発行システムの機能を表すブロック図である。

【図11】 ICカードの構成を表す図である。

【図12】 証明書発行装置の機能を表すブロック図である。

【図13】 証明書発行装置の動作を表すフローチャートである。

【図14】 多機能情報端末の仕組みを表す図である。

【符号の説明】

1 証明書発行システム

2 端末

2' 証明書発行装置

2'' 多機能情報端末

3 記録媒体

4 証明書管理サーバ

5 ネットワーク

7 店舗のレジ内

20 バスライン

21 中央演算処理装置 (CPU)

22 メモリ

23 通信部

26 識別情報読み取り手段

27 識別情報送信手段

28 真偽受信手段

28' 真偽確認手段

29 証明書発行手段

31 記録媒体

32 識別情報

33 真偽情報

41、41' 識別情報データベース

42 識別情報受信手段

43 真偽判定手段

44 真偽送信手段

200 印刷装置

200' 記録媒体読み取り／書き込み装置

201 印刷部

202 通信部

203 計算機

204 識別情報読み取り部

311 ICモジュール

312 端子

313 ICチップ

フロントページの続き

(51) Int. Cl. ⁷	識別記号	F I	(参考)
G 0 6 F 17/60	5 0 2	G 0 6 F 17/60	5 0 2
	5 1 0		5 1 0
B 4 2 D 15/10	5 2 1	B 4 2 D 15/10	5 2 1
G 0 6 K 17/00		G 0 6 K 17/00	L
			S
19/00		19/00	Q